MASTER EN SCIENCES MATHÉMATIQUES À FINALITÉ APPROFONDIE

La théorie de Galois aujourd'hui

Baptise, Martin

Award date:
2021

Awarding institution:
Universite de Namur

Université de Namur

Faculté des Sciences

La théorie de Galois aujourd'hui

**Mémoire présenté pour l'obtention
du grade académique de master en Sciences
Mathématiques, à finalité approfondie**

Martin Baptiste

Promoteur
Pr. Alexandre Mauroy

25 mai 2021

1 Préface

Ce mémoire s'inscrit davantage comme un résumé non-exhaustif des différents sujets dans lesquels la théorie de Galois interfère que comme une véritable présentation rigoureuse de toute cette théorie. Le premier chapitre est consacré à la théorie de Galois classique, celle développée par Galois, mais sous sa forme moderne. Ce dernier est plus complet que les chapitres suivants car il est à la base de tous ceux qui le succèdent. L'objectif visé est de formuler une présentation plus simple que ce que l'on peut trouver dans les livres ou dans les cours connus de cette théorie et de démystifier certains points pour les néophytes. Ainsi, j'espère exposer une approche que j'aurais aimé avoir lue lors de mes premiers contacts avec la théorie de Galois. Le deuxième chapitre est consacré à la théorie de Galois infinie, un premier prolongement de la théorie de Galois classique aux extensions algébriques de degré infini. Cette théorie, pourtant importante, est assez peu exposée dans les livres sur la théorie de Galois et le but de cette section est de coupler la théorie quelque peu abstraite avec des exemples assez concrets. Le troisième exhibe les liens entre l'arithmétique des extensions de $\mathbb{Q}$ et le groupe de Galois associé. Ce chapitre explicite comment la théorie de Galois s'inscrit naturellement dans une théorie plus ancienne qu'elle : La théorie des nombres. Le quatrième présente succinctement la théorie de Galois différentielle. Celle-ci possède de nombreuses analogies avec le premier chapitre mais l'objet principal de cette section est l'équation différentielle linéaire. Le cinquième chapitre porte sur la théorie de Galois des revêtements, une théorie qui montre qu'il existe une correspondance galoisienne entre revêtements et sous-groupes du groupe fondamental de l'espace topologique de base.

Si le chapitre 3 semble assez court, il est, avec la théorie de Galois classique, celui qui m'a demandé le plus de temps à étudier et à digérer. Ce dernier a littéralement décentré mon point de vue général des mathématiques et j'y ai découvert une magnifique théorie, riche de connexions et d'interprétations pour l'algèbre, l'analyse, la topologie et la théorie des nombres. Vous l'aurez compris, la théorie algébrique des nombres, de par son histoire, est une théorie gigantesque. Ce chapitre ne représente donc qu'une infime partie qui, je l'espère, se suffit à elle-même. Du reste, les deux derniers chapitres, encore plus courts, ne sont pas à la hauteur de ce que j'avais envisagé. Les démonstrations de la théorie de Galois différentielle nécessitent un certain nombre de notions de la géométrie algébrique que je n'ai pas eu le temps de maîtriser. Le chapitre sur les revêtements se voit, lui aussi, tronqué par le temps malgré ma lecture attentive de quelques ouvrages du domaine.

Mots-clefs : Théorie de Galois, théorie de Galois infinie, topologie algébrique, théorie algébrique des nombres, théorie de Galois différentielle.

2 Remerciements

Le choix même de ce sujet comme travail final de mes études m'aurait été impossible sans mon promoteur Alexandre Mauroy. Je le remercie pour la confiance

qu'il m'a accordée. Je lui suis reconnaissant pour ses relectures, pour l'autonomie qu'il m'a laissée, pour ces encouragements, mais aussi pour avoir su délimiter et recentrer l'objectif du mémoire avant que je ne m'engage dans une direction inéluctablement succincte et abstraite.

Je remercie ensuite Cédric Simal pour sa lecture attentive de ce pavé. Ses conseils et ses astuces m'ont été utiles pour corriger certaines erreurs et parfaire l'illustration générale. Son point de vue externe m'a permis de modifier certains points abscons.

Du reste, il m'est impossible de ne pas mentionner ma famille, mes proches et en particulier celle qui m'a soutenu au quotidien.

Les erreurs restantes du mémoire sont miennes.

Table des matières

3 Théorie de Galois classique

La construction de ce chapitre se base sur plusieurs ouvrages. Pour une approche lente mais pédagogique (on y atteint le théorème fondamental de la théorie de Galois après plus de 90 pages) on a [10],[26],[31],[32]. Pour une présentation plus complète (mais plus rapide) qui dépasse le cadre de la théorie classique il y a [14],[21],[22],[37],[17] (le premier et le dernier sont en français, il y en a une myriade d'autres). Pour un retour aux sources, le mémoire de Galois est disponible en ligne : voir [8]. Pour l'oeuvre très connue d'Emil Artin, (sur laquelle beaucoup se sont basés pour écrire leurs cours sur la théorie de Galois classique) il y a le fameux [3].

3.1 Introduction

On trouvera plus d'information sur la vie d'Evariste Galois dans [33].

Évariste Galois (1811-1832) est un mathématicien français connu à la fois pour ses travaux en algèbre mais aussi pour sa vie qui fût particulièrement courte et tumultueuse. Si Galois est présenté comme le Rimbaud des mathématiques, celui-ci n'est pas parti faire de la contrebande en Afrique après avoir terminé son oeuvre. En effet, ce dernier est mort à 20 ans (dans un duel improbable), avant même de se faire connaître de ses contemporains. Cependant, rien d'abracadabrantesque dans son travail ; c'est aujourd'hui un emblème des mathématiques.

Grand lecteur de Gauss (1777-1855), sa théorie trouve son inspiration dans "Disquisitiones arithmeticae" ainsi que dans la théorie des groupes et des équations algébriques de Lagrange (1736-1813). La théorie de Galois telle qu'elle est enseignée aujourd'hui est née au fil des années et des contributions de nombreux savants, bien après la mort de Galois. L'originale se trouve dans une lettre adressée à son ami Auguste Chevalier (1809-1868), rédigée dans les derniers jours avant son décès (d'une balle dans le ventre, pendant le duel fatal). Avant cela, et après que son manuscrit ait été perdu par l'académie des sciences, Galois tentera de présenter son mémoire à de grands mathématiciens comme Poisson (1781-1840) ou Fourier (1768-1830), mais sans succès car le premier ne voyait là qu'un résultat confus et similaire au mémoire d'Abel (1802-1829) et le second décèdera avant de l'avoir lu. Incompris de son vivant, il faudra attendre près de 15 ans pour que sa théorie soit présentée dans le Journal de Liouville, et ce grâce aux efforts de son ami Auguste et de son frère Alfred Galois. Cependant, avec l'impulsion des travaux de Sophus Lie (1842-1899), ce n'est que vers la fin du 19-ième siècle que sa théorie est reconnue, non pas comme simple apport parmi d'autres à la théorie des équations algébriques, mais bien comme un résultat centrale de l'algèbre moderne. Finalement, ce sont des mathématiciens comme Emil Artin (1898-1962) qui moderniseront l'expression générale de cette théorie afin que celle-ci soit utilisée aussi bien dans les recherches contemporaines que pour faciliter son enseignement.

En termes modernes, l'objectif initial de la théorie de Galois est de donner une condition nécessaire et suffisante pour qu'une équation polynomiale

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 = 0$$

soit résoluble par radicaux. Par définition, la résolubilité par radicaux revient à se demander s'il est possible d'exprimer les racines de f en termes de combinaisons de produits, sommes, différences, quotients ou racines k-ième des coefficients de f. Pour le degré 2 il est bien connu que le polynôme $aX^2 + bX + c$ possède les racines

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a},$$

et que cette formule fonctionne pour tout $a, b, c \in \mathbb{C}$ et $a \neq 0$. Au vu de l'expression des racines, il est clair que tout polynôme de degré 2 est résoluble par radicaux. Il existe des formules similaires pour les polynômes de degré 3 et 4 ce qui fait de ces derniers des polynômes résolubles par radicaux. Pour le degré 5 le problème se complexifie. Évidemment, pour un polynôme donné de degré quelconque avec des coefficients bien choisis, il est toujours possible de déterminer les racines de manière exacte. Cependant, et c'est le résultat du théorème d'Abel-Ruffini, pour un polynôme générique de degré au moins 5 il n'existe pas d'expression par radicaux pour exprimer ses racines. Ainsi, il est parfois possible de résoudre un polynôme de degré 5 par radicaux, par exemple

$$X^5 - 15X^4 + 85X^3 - 225X^2 + 274X - 120 = (X-1)(X-2)(X-3)(X-4)(X-5),$$

mais parfois pas, par exemple pour [1]

$$X^5 - 4X + 2.$$

La condition nécessaire et suffisante de résolubilité par radicaux de la théorie de Galois nous dit qu'un polynôme est résoluble par radicaux si et seulement si son groupe de Galois est résoluble. Ainsi, la différence entre les deux polynômes précédents est que le premier possède un groupe de Galois résoluble tandis que le second pas. Le théorème de Galois est par conséquent un résultat plus précis que celui d'Abel-Ruffini. Mais sa théorie ne s'arrête pas là. En effet, il y a un autre théorème, plus fondamental encore, qui définit une bijection entre l'ensemble des sous-groupes du groupe de Galois et l'ensemble des corps intermédiaires à deux corps définis par le polynôme considéré. De manière plus abstraite, la théorie de Galois est un outil puissant pour étudier la théorie des corps par la théorie des groupes.

Aujourd'hui la théorie de Galois classique s'étudie en plusieurs étapes. Celle-ci nécessite des connaissances en théorie des groupes (avec les notions d'ordre, de sous-groupe, de classe d'équivalence, de groupe quotient, d'homomorphisme de groupes etc...) en théorie des anneaux (avec les idéaux, l'intégrité, les anneaux quotients ainsi que les homomorphismes d'anneaux, les théorèmes d'isomorphismes etc...) et puis il faut une certaine familiarité avec les polynômes. Nous pensons qu'il est utile d'avoir une vision assez globale de la théorie des corps pour comprendre le décor général et voir pourquoi la théorie de Galois déborde et échappe à son objectif initial qui était restreint à la résolution des équations algébriques.

Nous présenterons donc la théorie de Galois classique en suivant les étapes suivantes : D'abord des rappels généraux sur les corps, les anneaux et les polynômes. Ensuite nous démontrerons les propriétés générales des extensions algébriques. Après cela, nous serons en mesure de définir le groupe de Galois d'une extension et d'exposer les lemmes et les théorèmes nécessaires à la démonstration de la correspondance galoisienne (théorème fondamental de la théorie de Galois). Le reste du chapitre est une succession d'applications non exhaustive. Parmis celle-ci on compte : les extensions cyclotomiques, les extensions cycliques, la résolubilité par radicaux et la construction à la règle et au compas.

3.2 Rappels sur les corps et les polynômes

Cette section ne concerne que des rappels. Commençons par définir l'objet principal de la section.

Définition 3.1. Un corps est un anneau commutatif unitaire tel que tout élément non nul est inversible.

Example 3.1. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des corps pour les opérations d'addition et de multiplication usuelles.

1. Voir l'exemple 3.89

Par la suite nous ne rencontrerons que des corps commutatifs, c'est-à-dire des corps tels que la seconde loi de composition interne est commutative (en l'occurrence la multiplication usuelle pour les corps qui nous intéressent). Nous désignerons par "corps" tout corps commutatif. De même, les anneaux considérés sont toujours unitaires. Afin d'éviter les répétitions inutiles, nous utiliserons le terme "anneau" pour désigner tout anneau unitaire.

Définition 3.2. Un anneau commutatif A est intègre si pour tout $a, b \in A$ on a $ab = 0 \implies a = 0$ ou $b = 0$.

L'intégrité d'un corps est automatique. En effet, si a, b sont des éléments non nuls d'un corps alors $ab = 0$ implique que $0 = abb^{-1} = a$ ce qui contredit l'hypothèse. À partir d'un anneau commutatif intègre on peut construire un corps appelé corps des fractions de cet anneau.

Définition 3.3. Le corps des fractions d'un anneau commutatif intègre A est défini et noté

$$Frac(A) = \left\{ ab^{-1} \mid a, b \in A \text{ et } b \neq 0 \right\}.$$

Cet objet est bien défini, la preuve est omise.

Définition 3.4. Un idéal I de l'anneau commutatif A est un sous-groupe additif de A tel que pour tout $x \in I$ et pour tout $a \in A$ on a $xa \in I$.

Un idéal est dit trivial si $I = A$ ou $I = 0$. Un idéal est dit principal s'il est généré par un seul élément. Dans ce cas nous noterons $\langle a \rangle$ l'idéal généré par l'élément $a \in A$.. Si A ne possède que des idéaux principaux on dit que A est un anneau principal.

Example 3.2. Les idéaux de l'anneau $(\mathbb{Z}, +, .)$ sont les sous-ensembles $n\mathbb{Z} = \{\text{multiples de n}\}$ pour tout $n \in \mathbb{Z}$. Tous ces idéaux sont principaux, par conséquent $\mathbb{Z}$ est un anneau principal.

Définition 3.5. Un idéal est dit $M \subseteq A$ est dit maximal s'il n'est contenu dans aucun idéal propre de A.

La propriété importante des idéaux premiers est que A/M est toujours un corps.

Proposition 3.3. *Les idéaux d'un corps sont triviaux.*

Démonstration. Soit I un idéal d'un corps K. Si $I = \{0\}$ il n'y a rien à montrer. Supposons que $I \neq \{0\}$. Si $a \in I$ est non nul, alors il existe $a^{-1} \in K$. Par conséquent $a^{-1}a = 1 \in I$. Dès lors $I = KI = K$. □

Définition 3.6. Soient A et B deux anneaux. Un homomorphisme d'anneaux $\varphi : A \to B$ est une fonction vérifiant

— $\varphi(ab) = \varphi(a)\varphi(b)$
— $\varphi(a + b) = \varphi(a) + \varphi(b)$

— $\varphi(1_A) = 1_B$
pour tout $a, b \in A$.

On parle d'homomorphisme de corps lorsque A et B sont des corps. Le noyau d'un homomorphisme d'anneaux commutatifs est un idéal. En particulier, lorsque A est un corps on voit par la propriété 3.3 que $Ker(\varphi) = \{0\}$. Le résultat suivant découle directement de cette observation.

Proposition 3.4. *Tout homomorphisme de corps est un injectif.*

3.2.1 Caractéristique d'un corps

Soit K un corps, 1_K son élément neutre pour la multiplication, et soit l'homomorphisme d'anneaux

$$\varphi : \mathbb{Z} \to K : n \mapsto n.1_K = \underbrace{1_K + \cdots + 1_K}_{n}.$$

La caractéristique de K, notée Car(K), est définie comme suit. Si Ker(φ)=$\{0\}$ alors K est dit de caractéristique 0. Sinon, comme $\mathbb{Z}$ est un anneau principal, il existe un entier positif $n > 0$ tel que Ker(φ)=$n\mathbb{Z}$ et K est dit de caractéristique n. Si Car(K)=0, alors φ est injectif et $\mathbb{Z}$ s'identifie à un sous-anneau intègre $\varphi(\mathbb{Z})$ de K. Le corps des fractions de $\varphi(\mathbb{Z})$ est le plus petit sous-corps de K, il est isomorphe au corps des fractions $\mathbb{Q}$ de $\mathbb{Z}$. En conséquence, le cardinal de K est infini. Comme K est intègre, si Car(K)=n, alors n est un nombre premier. En effet, supposons qu'il existe deux entiers $1 < a, b < n$ tels que $n = ab$. Alors

$$0 = n.1_K = (ab).1_K = (a.1_K).(b.1_K),$$

donc $a.1_K = 0$ ou $b.1_K = 0$, ce qui contredit la minimalité de n tel que Ker(φ)=$n\mathbb{Z}$. Dans ce cas, $\mathbb{Z}/n\mathbb{Z}$ est isomorphe au plus petit sous-corps de K. Comme tout corps de caractéristique 0 est infini, tout corps fini est de caractéristique $p > 0$. Il existe cependant des corps de caractéristique $p > 0$ mais de cardinal infini. On peut citer par exemple $\mathbb{F}_p((t))$ le corps des séries de Laurent à coefficients dans $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Du fait qu'ils ne contiennent pas de corps plus petits qu'eux, les corps $\mathbb{Q}$ et $\mathbb{F}_p$ sont appelés des corps premiers. Leur place est donc objectivement centrale. La théorie de Galois se veut la plus générale possible, il sera cependant pertinent de distinguer ces corps car ceux-ci ne se comportent pas toujours de la même manière. Par la suite, lorsque la caractéristique du corps en question n'est pas précisée, le lecteur peut supposer le résultat indépendant de celle-ci.

Remarque 3.5. Soient x et y des éléments d'un corps K. La grande différence entre un corps de caractéristique p et un corps de caractéristique 0 est que dans le premier

$$(x + y)^p = x^p + y^p,$$

tandis que dans le second on a la formule classique du binôme de Newton

$$(x + y)^p = \sum_{k=0}^{p} C_p^k x^k y^{p-k}.$$

Pour expliquer cela, supposons que $\mathrm{Car}(K) = p$. En développant $(x+y)^p$ on retrouve la formule de Newton mais pour chaque $1 < k < p$ on voit que

$$C_p^k = \frac{p!}{(p-k)!k!} \in \mathbb{Z}$$

possède un numérateur divisible par p et un dénominateur premier à p. Par conséquent $p|C_p^k$ pour tout $1 < k < p$. Comme la caractéristique de K est p, ces éléments sont donc nuls dans K d'où la conclusion.

Une des conséquences directes de cette remarque est la proposition suivante.

Proposition 3.6. *Soit K un corps de caractéristique p. L'application dite de Frobenius $\Phi : K \to K : x \mapsto x^p$ est un homomorphisme de corps.*

Démonstration. Soient $x, y \in K$. Par la remarque précédente

$$\Phi(x+y) = (x+y)^p = x^p + y^p = \Phi(x) + \Phi(y).$$

De plus $\Phi(xy) = x^p y^p = \Phi(x)\Phi(y)$ et $\Phi(1) = 1^p = 1$. Finalement $\mathrm{Ker}(\Phi) = \{0\}$ donc Φ est un homomorphisme de corps dont l'image est $K^p = \{x^p \mid x \in K\}$. □

Pour justifier la remarque sur la commutativité des corps on a le théorème de Wedderburn.

Théorème 3.7. *Les corps finis sont des corps commutatifs.*

3.2.2 Anneaux des polynômes

Avec les corps, les polynômes font partis des objets centraux de la théorie de Galois classique. Nous avons l'habitude de travailler avec les polynômes à coefficients dans $\mathbb{R}$ ou dans $\mathbb{C}$ depuis les secondaires. Cependant, la théorie de Galois tire sa richesse des relations entre le plus petit corps contenant les coefficients du polynôme et le plus petit corps contenant ce corps ainsi que les racines du polynôme en question. Pour gagner en généralité, il est intéressant d'étudier les polynômes à coefficients dans un corps K quelconque.

Définition 3.7. L'anneau des polynômes d'inconnue X et à coefficients dans un corps K est noté $K[X]$.

Il est clair que $K[X]$ forme un anneau commutatif. Un élément $f(X) \in K[X]$ est de la forme

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0,$$

où $a_i \in K$ pour tout $i = 0, \ldots, n$ et $a_n \neq 0$ de sorte que $\deg(f(X)) = n$. Le degré d'un polynôme vérifie $\deg(f(X)g(X)) = \deg(f(X)) + \deg(g(X))$ pour tout $f(X), g(X) \in K[X]$. Comme K est un corps, il est intègre et $K[X]$ hérite de cette propriété. De plus $K[X]$ est un anneau euclidien pour la fonction euclidienne

$$\phi(f(X)) = \begin{cases} \phi(f(X)) = \deg(f(X)) \text{ si } f(X) \neq 0 \\ \phi(f(X)) = -1 \text{ si } f(X) = 0, \end{cases}$$

c'est à dire que si $g(X) \in K[X]$ est un polynôme non nul alors il existe $r(X) \in K[X]$ tel que

$$f(X) = g(X)h(X) + r(X)$$

avec $\phi(r(X)) < \phi(g(X))$. Cette division euclidienne est unique.

Comme $K[X]$ est un anneau euclidien, c'est aussi un anneau principal. Ses idéaux sont donc principaux et on note $\langle f(X) \rangle = \{f(X)g(X) \mid g(X) \in K[X]\}$ l'idéal principal généré par $f(X)$. L'ensemble des éléments inversibles de $K[X]$ est

$$K^* = \{x \in K \mid x \neq 0\}.$$

Définition 3.8. Un polynôme non constant $p(X) \in K[X]$ est irréductible si $p(X) = f(X)g(X)$ pour $f(X), g(X) \in K[X] \implies f(X) \in K^*$ ou $g(X) \in K^*$.

Par abus de langage, on peut aussi dire que $p(X)$ est irréductible sur K ou dans K. Rappelons aussi que tout anneau principal est factoriel. De ce fait, les éléments de $K[X]$ se factorisent de manière unique en un produit de polynômes irréductibles $p_1(X), \ldots, p_n(X) \in K[X]$ et d'un élément inversible $u \in K^*$ de telle façon que

$$f(X) = up_1(X) \ldots p_n(X).$$

Remarque 3.8. Les polynômes de degré 1, c'est à dire de la forme $f(X) = \alpha X + \beta$ avec $\alpha, \beta \in K$, sont irréductibles dans $K[X]$ car sinon il existerait $g(X), h(X) \in K[X] \setminus K^*$ tel que $f(X) = g(X)h(X)$ et

$$1 = \deg(f(X)) = \deg(g(X)) + \deg(h(X)) \geq 2$$

ce qui est impossible.

Example 3.9. Le polynôme

$$X^2 - 2$$

est irréductible dans $\mathbb{Q}$ car $\pm\sqrt{2} \notin \mathbb{Q}$ mais il ne l'est pas dans $\mathbb{R}$ car

$$X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2}).$$

Le polynôme

$$X^2 + X + 1$$

est irréductible sur $\mathbb{R}$ mais

$$X^2 + X + 1 = (X - e^{\frac{2i\pi}{3}})(X - e^{\frac{4i\pi}{3}})$$

dans $\mathbb{C}$.

Pour un polynôme de degré strictement supérieur à 1, il existe des critères permettant de déterminer si celui-ci est irréductible ou non. On a par exemple le critère d'Eisenstein.

Théorème 3.10. *(Critère d'Eisenstein dans $\mathbb{Q}$) Soit $f(X) \in \mathbb{Q}[X]$ un polynôme non nul de la forme*

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0,$$

tel qu'il existe un nombre premier p satisfaisant
- *$p | a_i$ pour $i = 0, \ldots, n-1$*
- *$p \nmid a_n$*
- *$p^2 \nmid a_0$.*

Alors $f(X)$ est irréductible sur K.

Démonstration. La preuve peut être trouvée dans REF. □

Il existe une version plus générale fonctionnant pour n'importe quel corps K mais faisant intervenir la notion d'anneaux des entiers. Nous n'en aurons pas l'utilité dans notre exposé.

Example 3.11. Le polynôme $X^5 + 18X + 3$ est irréductible sur $\mathbb{Q}$ car 3 ne divise pas le coefficient de $3 \nmid 1$, $3|18$ et $3|3$ et $3^2 \nmid 3$.

Remarque 3.12. Le critère d'Eisenstein peut ne pas fonctionner directement. Il faut parfois user d'un changement de variable pour pouvoir l'utiliser. Soit le polynôme $f(X) = X^4 + X^3 + X^2 + X + 1$. Le critère d'Eisenstein ne s'applique pas. Cependant si on pose $X = Y + 1$ on a

$$f(Y + 1) = Y^5 + 5Y^3 + 10Y^2 + 10Y + 5$$

et on remarque que 5 satisfait aux hypothèses du critère d'Eisenstein. Le changement de variable ne modifiant pas l'irrationalité des racines, on en conclut que $f(X)$ est irréductible sur $\mathbb{Q}$. Les bons changements de variable à tester se trouvent parmi les diviseurs du discriminant du polynôme.

Proposition 3.13. *Soit $f(X) \in K[X]$ et $\alpha \in K$, alors*

$$f(\alpha) = 0 \iff (X - \alpha) \text{ divise } f(X).$$

Démonstration. Si $(X - \alpha)$ divise $f(X)$ alors il existe $g(X) \in K[X]$ tel que $f(X) = (X - \alpha)g(X)$ donc $f(\alpha) = 0$. Si $f(\alpha) = 0$ alors par la division Euclidienne

$$f(X) = (X - \alpha)g(X) + r(X)$$

avec $f(\alpha) = r(\alpha) = 0$ et $r(X) \in K^*$ d'où $r(X) = 0$ et $(X - \alpha)$ divise $f(X)$. □

Proposition 3.14. *Soit A un anneau intègre principal et $p \in A$ non nul et non inversible, alors $\langle p \rangle$ est un idéal maximal si et seulement si p est un élément irréductible.*

Démonstration. Si p est irréductible alors $p = ab$ pour $a, b \in A$ implique que $a \in A^*$ ou $b \in A^*$ est un élément inversible. Donc les seuls idéaux propres de A contenant $\langle p \rangle$ sont de la forme $\langle \epsilon p \rangle$ où $\epsilon \in A^*$. Or comme $\epsilon \in A^*$, $\langle p \rangle = \langle \epsilon p \rangle$, donc $\langle p \rangle$ est un idéal maximal. Inversement, si p n'est pas irréductible alors il existe $a, b \in A \setminus A^*$ non nuls tels que $p = ab$. Dès lors $\langle p \rangle \subset \langle b \rangle \subset A$ et $\langle p \rangle$ n'est pas un idéal maximal. □

Corollaire 3.15. *Soit $p(X) \in K[X]$ un polynôme irréductible sur $K[X]$. Alors*

$$K[X]/\langle p(X)\rangle$$

est un corps.

Démonstration. Comme $K[X]$ est un anneau intègre principal et que $p(X)$ est irréductible, par la propriété 3.14, $\langle p(X)\rangle$ est un idéal maximal, donc $K[X]/\langle p(X)\rangle$ est un corps. □

Ce corps $K[X]/\langle p(X)\rangle$ est formé des restes de la division euclidienne des polynômes de $K[X]$ par $p(X)$. La projection canonique

$$\pi : K[X] \to K[X]/\langle p(X)\rangle$$

est donc définie par

$$\pi : f(X) = q(X)p(X) + r(X) \mapsto \pi(f(X)) = r(X) + \langle p(X)\rangle.$$

Ses éléments sont des polynômes de degré inférieur strictement au degré de $p(X)$. Pour ne pas alourdir l'écriture, si $\alpha \in K$ alors $\pi(\alpha)$ est encore noté α de sorte que la classe de polynômes $\pi(f(X)) = a_nX^n + \cdots + a_1X + a_0 + \langle p(X)\rangle$ n'est pas notée

$$(a_n + \langle p(X)\rangle)X^n + \cdots + (a_1 + \langle p(X)\rangle)X + (a_0 + \langle p(X)\rangle) + \langle p(X)\rangle.$$

Ce corps est muni des lois d'addition et de multiplication modulo $p(X)$.

Example 3.16. Posons $K = \mathbb{Q}$ et $f(X) = X+7 \in \mathbb{Q}[X]$. Alors $\mathbb{Q}/\langle X+7\rangle$ est un corps. Tous ses éléments sont des polynômes constants. De plus, si $a \in \mathbb{Q} \subset \mathbb{Q}[X]$ alors $\pi(a) = a + \langle f(X)\rangle := a$, donc $\mathbb{Q}/\langle X + 7\rangle \cong \mathbb{Q}$.

Example 3.17. Prenons à nouveau $K = \mathbb{Q}$, $f(X) = X^2 + 5X + 1 \in \mathbb{Q}[X]$ est irréductible sur $\mathbb{Q}[X]$. Donc $Q[X]/\langle X^2 + 5X + 1\rangle$ est un corps. L'élément $g(X) = X^3 + 6X^2 + 6X + 1 \in Q[X]$ se factorise comme $g(X) = (X + 1)f(X)$ donc $\pi(g(X)) = 0 + \langle f(X)\rangle \in \mathbb{Q}[X]/\langle X^2 + 5X + 1\rangle$. Le polynôme $h(X) = X^3$ se factorise comme $h(X) = (X - 5)f(X) + 24X + 5$ d'où $\pi(h(X)) = 24X + 5 + \langle f(X)\rangle \in \mathbb{Q}[X]/\langle X^2 + 5X + 1\rangle$.

3.3 Extension de corps

Définition 3.9. Une extension de corps $L \supseteq K$ est un corps qui contient K comme sous-corps.

Remarque 3.18. Certains auteurs définissent une extension L de K comme un corps tel qu'il existe un homomorphisme de corps $i : K \to L$. Or, par la propriété 3.4, i est injectif. Cette définition est donc équivalente à la première puisque l'injection de K dans L signifie que K est isomorphe à un sous-corps de L.

Dans la définition 3.9 le corps K est appelé le corps de base. Lorsqu'il est utile de préciser ce dernier, on note l'extension L/K. Le corps L peut être vu comme un K-espace vectoriel et, en tant que tel, sa dimension, qu'on appelle degré, est notée $[L : K]$.

Définition 3.10. Une extension L/K est finie si $[L : K] < +\infty$.

Comme nous le verrons, celle-ci n'est pas nécessairement finie et dépendra du nombre d'éléments adjoints au corps de base ainsi que de leur nature.

Remarque 3.19. Il est important de voir que tout corps est, en particulier, soit une extension de $\mathbb{Q}$ soit une extension de $\mathbb{F}_p$. Ceci découle du paragraphe dédié à la caractéristique d'un corps.

Définition 3.11. Soit L/K un extension et $S \subset L$ un sous-ensemble (éventuellement infini) de L. On note $K[S]$ le sous-anneau de L généré par K et S. De même, on écrit $K(S)$ le sous-corps de L généré par K et S.

De manière équivalente, $K(S)$ est l'intersection de tous les sous-corps de L contenant à la fois K et S, ou encore, c'est le plus petit sous-corps de L contenant K et S. C'est donc une extension de K dans L. Si $S = \{\alpha_1, \ldots, \alpha_n\}$ alors l'extension est notée $K(\alpha_1, \ldots, \alpha_n)$. L'adjonction des n éléments α_i peut se faire en n étapes, dans n'importe quel ordre. Ainsi

$$K(S) = K(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n) = K(\alpha_1)(\alpha_2) \ldots (\alpha_{n-1})(\alpha_n)$$

et par exemple pour $n = 2$,

$$K(\alpha_1, \alpha_2) = K(\alpha_1)(\alpha_2) = K(\alpha_2)(\alpha_1) = K(\alpha_2, \alpha_1).$$

Définition 3.12. L'extension L/K est finiment générée sur K s'il existe un sous-ensemble fini $S \subset L$ tel que $L = K(S)$.

Comme il a été dit, en général, $n \neq [K(\alpha_1, \ldots, \alpha_n) : K]$ car cela dépend du "genre" de nombres que sont $\alpha_1, \ldots, \alpha_n$ par rapport au corps de base K.

Les notations pour les anneaux fonctionnent de la même façon que pour les corps. Si $S \subset L$ l'anneau $K[S]$ est aussi l'intersection de tous les sous-anneaux de L contenant K et S ou encore le plus petit sous-anneau de L contenant K et S. Si $S = (\alpha_1, \ldots, \alpha_n)$ l'anneau est noté $K[S] = K[\alpha_1, \ldots, \alpha_n]$ et

$$K[S] = K[\alpha_1, \ldots, \alpha_{n-1}][\alpha_n] = K[\alpha_1][\alpha_2] \ldots [\alpha_{n-1}][\alpha_n].$$

L'exemple suivant illustre bien le cas générique des extensions que nous serons amenés à considérer.

Example 3.20. Soit $a \in \mathbb{C}$, $a \neq 0$. Le corps $\mathbb{Q}(a)$ est une extension de $\mathbb{Q}$. En outre, $a \in \mathbb{Q}(a)$ et comme $\mathbb{Q}(a)$ est un corps nous savons que $a^n \in \mathbb{Q}(a)$ pour tout $n \in \mathbb{Z}$. En considérant toutes les combinaisons possibles des a^n avec les éléments de $\mathbb{Q}$,

$$\mathbb{Q}(a) = \left\{ \frac{p(a)}{q(a)} \;\middle|\; p(X), q(X) \in \mathbb{Q}[X] \text{ et } q(a) \neq 0 \right\}.$$

En particulier, si $a = \sqrt{2}$, ce corps se réduit à

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

qui est un $\mathbb{Q}$-espace vectoriel de dimension 2. Si on adjoint $\sqrt{3}$ à ce corps nous obtenons l'extension

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}$$

qui est une extension de $\mathbb{Q}(\sqrt{2})$ et donc de $\mathbb{Q}$. Sa dimension sur $\mathbb{Q}$ est 4 alors que sa dimension sur $\mathbb{Q}(\sqrt{2})$ est 2. Notons que

$$4 = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \times 2.$$

De plus, $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}(\sqrt{3}) = \mathbb{Q}[\sqrt{3}]$ et $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$.

Proposition 3.21. *Soit L/K et $\alpha_1, \ldots, \alpha_n \in L$. Posons $\alpha = (\alpha_1, \ldots, \alpha_n)$. La fonction*

$$\psi_\alpha : K[X_1, \ldots, X_n] \to K[\alpha_1, \ldots, \alpha_n] : f(X_1, \ldots, X_n) \mapsto f(\alpha_1, \ldots, \alpha_n),$$

est un homomorphisme d'anneaux surjectif.

Démonstration. La fonction ψ_α est bien définie en ce sens que si $f(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$ alors $\psi_\alpha(f(X_1, \ldots, X_n)) = f(\alpha_1, \ldots, \alpha_n)$ est dans $K[\alpha_1, \ldots, \alpha_n]$. En effet, $\psi_\alpha(X_i) = \alpha_i \in K[\alpha_1, \ldots, \alpha_n]$ pour tout $1 \leq i \leq n$ et comme $K[\alpha_1, \ldots, \alpha_n]$ est un anneau contenant K, $\psi_\alpha(f(X_1, \ldots, X_n)) = f(\alpha_1, \ldots, \alpha_n) \in K[\alpha_1, \ldots, \alpha_n]$. On a donc

$$\mathrm{Im}(\psi_\alpha) = \{f(\alpha_1, \ldots, \alpha_n) \mid f \in K[X_1, \ldots, X_n]\} \subseteq K[\alpha_1, \ldots, \alpha_n].$$

Ensuite il est clair que $\psi_\alpha(1) = 1$ et que si $f(\mathbf{X}) := f(X_1, \ldots, X_n)$ et $g(\mathbf{X}) := g(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$ alors

$$\psi_\alpha(f(\mathbf{X}) + g(\mathbf{X})) = f(\alpha) + g(\alpha) = \psi_\alpha(f(\mathbf{X})) + \psi_\alpha(g(\mathbf{X})),$$

et

$$\psi_\alpha(f(\mathbf{X})g(\mathbf{X})) = f(\alpha)g(\alpha) = \psi_\alpha(f(\mathbf{X}))\psi_\alpha(g(\mathbf{X})).$$

Donc ψ_α est un homomorphisme d'anneaux.

Finalement, il reste à voir que

$$K[\alpha_1, \ldots, \alpha_n] \subseteq \mathrm{Im}(\psi_\alpha) = \{f(\alpha_1, \ldots, \alpha_n) \mid f \in K[X_1, \ldots, X_n]\}$$

pour obtenir la surjectivité de ψ_α. Mais cela résulte du fait que $K[\alpha_1, \ldots, \alpha_n]$ est, par définition, le plus petit sous-anneau de L contenant $\alpha_1, \ldots, \alpha_n$ et que $\mathrm{Im}(\psi_\alpha)$ est un anneau (car image par un homomorphisme d'un anneau) contenant K et $\alpha_1, \ldots, \alpha_n$. □

Dans l'exemple 3.20 on exprime assez simplement l'extension $\mathbb{Q}(a)/\mathbb{Q}$ grâce aux polynômes et aux fractions rationnelles. Le corollaire suivant montre que cette construction est tout à fait générale.

Corollaire 3.22. *Soit L/K un extension de corps et $\alpha_1, \ldots, \alpha_n \in L$ tel que $A = K[\alpha_1, \ldots, \alpha_n]$ et $L = K(\alpha_1, \ldots, \alpha_n)$. Alors*

$$A = \{f(\alpha_1, \ldots, \alpha_n) \mid f \in K[X_1, \ldots, X_n]\}$$

et

$$L = \left\{ \frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)} \;\middle|\; f, g \in K[X_1, \ldots, X_n] \text{ et } g \neq 0 \right\}.$$

Succinctement,

$$L = \mathit{Frac}(A).$$

Démonstration. Le fait que $A = K[\alpha_1, \ldots, \alpha_n]$ a été démontré dans la proposition 3.21. Comme A est un sous-anneau de L, il est intègre. Par définition, le corps des fractions de A est le plus petit corps contenant A, d'où l'expression $L = \mathrm{Frac}(A)$. □

Le degré d'une extension peut s'obtenir en fonction des degrés des sous-extensions intermédiaires.

Théorème 3.23. *(Théorème de la base télescopique) Soit $K \subset L \subset E$ une tour d'extensions finies, alors*

$$[E : K] = [E : L][L : K].$$

Démonstration. Supposons que $[E : L] = n$ et $[L : K] = m$. Soient $(a_i)_{i \in J}$ une base de L/K et $(b_i)_{i \in I}$ une base de E/L. Si $x \in E$ alors il existe $c_1, c_2, \ldots, c_n \in L$ tel que $x = \sum_{i \in I} c_i b_i$. Or pour chaque c_i, il existe $d_{i1}, d_{i2}, \ldots, d_{im} \in K$ tel que $c_i = \sum_{j \in J} d_{ij} a_j$. Donc, on a

$$x = \sum_{i \in I} \big(\sum_{j \in J} d_{ij} a_j \big) b_i = \sum_{i \in I} \sum_{j \in J} d_{ij} (a_j b_i)$$

et les $n \times m$ éléments $(a_j b_i)_{i \in I, j \in J}$ forment un ensemble générateur de E/K. Il reste à montrer qu'ils sont linéairement indépendants. Supposons que

$$0 = \sum_i \sum_j d_{ij} a_j b_i,$$

comme $(b_i)_{i \in I}$ est une base de E/L et que $d_{ij} a_j \in L$ pour tout $i \in I$ et $j \in J$, on a $\sum_{i,j} d_{ij} a_j = 0$. Par le même argument, $(a_j)_{j \in J}$ est une base de L/K donc $d_{ij} = 0$ pour tout $i \in I, j \in J$. Par conséquent $(a_j b_i)_{i \in I, j \in J}$ est une base de E/K qui possède $n \times m$ éléments. □

Soit $f(X) \in K[X]$ un polynôme irréductible sur K. Alors il existe une extension L de K tel que $f(X)$ possède une racine dans L. Cette extension est construite par la proposition suivante.

Proposition 3.24. *Le corps $L = K[X]/\langle f(X)\rangle$ est une extension de K et $f(X)$ possède une racine dans L.*

Démonstration. Le corollaire 3.15 montre que $L = K[X]/\langle f(X)\rangle$ est un corps. Si $\alpha \in K$ alors la projection canonique $\pi : K[X] \to L$ restreinte à K est un homomorphisme de corps, donc est injective et L est une extension de K. L'image de X par π est une racine de $f(X)$ dans L car

$$\begin{aligned} 0 + \langle f(X)\rangle &= \pi(f(X)), \text{ car } f(X) \in \langle f(X)\rangle \\ &= f(\pi(X)) + \langle f(X)\rangle, \text{ car } \pi \text{ est un homomorphisme d'anneaux,} \end{aligned}$$

d'où l'assertion. □

Si cette proposition semble donner une construction des extensions assez abstraite, celle-ci va nous permettre par la suite de déduire des propriétés sur le degré et sur la base de L en tant que K-espace vectoriel. De plus, si K est un corps de caractéristique $p > 0$, alors on préférera utiliser ce résultat plutôt que le corollaire 3.22 pour expliciter l'extension L.

Example 3.25. Soit $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ le corps fini à deux éléments. Ces extensions ne sont pas de la forme $\mathbb{Z}/2^n\mathbb{Z}$ pour un certain $n \geq 2$ car ces anneaux ne sont pas des corps (ils ne sont même pas intègres). Les extensions de $\mathbb{F}_2$ ne sont pas non plus les $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ pour $p > 2$ premier car ces corps sont chacun des corps premiers (donc ne possédant pas de sous-corps). Pour illustrer cela, nous allons construire une extension de degré 2 de $\mathbb{F}_2$. La première chose à faire est donc de trouver un polynôme irréductible sur $\mathbb{F}_2$. Cherchons parmi les polynômes de degré ≤ 2. L'ensemble de ces polynômes est assez restreint. Les seuls éléments de $\mathbb{F}_2$ étant 0 et 1, les éléments de degré ≤ 2 de $\mathbb{F}_2[X]$ sont 0, 1, X, X^2, $1+X$, $1+X^2$, $X+X^2$ et finalement $1+X+X^2$. Clairement X, X^2 et $X+X^2$ ont 0 comme racine dans $\mathbb{F}_2$ (n'oublions pas que toutes les opérations sont réduites modulo 2), tandis que $1+X$, $1+X^2$ et $X+X^2$ ont 1 comme racine dans $\mathbb{F}_2$. Parmi ces polynômes on ne choisira pas ceux de degré 1 car sinon $\mathbb{F}_2 \cong F_2[X]/\langle X\rangle \cong F_2[X]/\langle 1+X\rangle$ sont des extensions triviales (ceci est déjà illustré dans l'exemple 3.16 et on peut facilement s'en convaincre pour $\mathbb{F}_2$). Le polynôme $f(X) = 1+X+X^2$ ne possédant pas de racines dans $\mathbb{F}_2$, il est le seul polynôme irréductible de degré 2 sur $\mathbb{F}_2[X]$. Par la proposition précédente $\mathbb{F}_2[X]/\langle f(X)\rangle$ est une extension de $\mathbb{F}_2$. Ses éléments sont les polynômes décrits précédemment, mais réduits modulo $f(X)$. Les éléments 0, 1, X, $X+1$ sont inchangés lors de la réduction modulo $f(X)$. Ensuite

$$\begin{aligned} X^2 &= X^2 + 2(X+1) \text{ car } 2X+2 = 0 \in \mathbb{F}_2[X] \\ &= X^2 + (X+1) + (X+1) \\ &= X + 1 + (X^2 + X + 1) \end{aligned}$$

donc $X^2 \equiv X+1 \bmod X^2+X+1$ puis $X^2+1 \equiv X \bmod X^2+X+1$ et $X^2+X \equiv 1 \bmod X^2+X+1$. Considérons la projection canonique $\pi : \mathbb{F}_2[X] \to \mathbb{F}_2[X]/\langle f(X)\rangle$ et notons $\pi(X) = \alpha$. Alors les seuls éléments de $\mathbb{F}_2[X]/\langle f(X)\rangle$

sont $\{0, 1, \alpha, \alpha+1\}$. Clairement $\mathbb{F}_2[X]/\langle f(X)\rangle = \{a + b\alpha \mid a, b \in \mathbb{F}_2\}$ qui est un espace vectoriel de dimension 2 sur $\mathbb{F}_2$. Notons que α est une racine de $X^2 + X + 1$ dans $\mathbb{F}_2[X]/\langle f(X)\rangle$ car $\alpha^2 = \alpha + 1$ ou encore $\alpha^2 - \alpha - 1 = 0$ c'est-à-dire $\alpha^2 + \alpha + 1 = 0$ (car $\alpha + 1 + \alpha + 1 = 2(\alpha + 1) = 0$ donc $\alpha + 1 = -\alpha - 1$). Pour terminer, remarquons que $\alpha + 1$ est aussi une racine de $X^2 + X + 1$ et comme ce polynôme est de degré 2, $\mathbb{F}_2[X]/\langle f(X)\rangle$ contient toutes les racines de $X^2 + X + 1$. Le corps obtenu est noté $\mathbb{F}_{2^2}$ ou $\mathbb{F}_4$ et s'appelle le corps fini à 4 éléments.

L'exemple précédent a permis de montrer comment construire un corps fini de 4 éléments à partir de $\mathbb{F}_2$. On pourrait se demander s'il est possible de construire un corps fini à 6 éléments. La réponse est non car tout corps fini est une extension finie d'un $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$, et donc, un espace vectoriel sur $\mathbb{Z}/p\mathbb{Z}$. Supposons que K soit une extension de degré n sur $\mathbb{Z}/p\mathbb{Z}$. Alors un élément de K est de la forme $\alpha = \alpha_1 x_1 + \cdots + \alpha_n x_n$ et il y a p^n combinaisons possibles pour les $\alpha_i \in \mathbb{F}_p$. Le cardinal de K est donc p^n. En conclusion, tout corps fini possède p^n éléments pour un certain nombre premier p et un certain $n \geq 1$.

Revenons au cas des corps quelconques. Avec les notations de la proposition 3.24, on montre qu'il existe une extension L/K contenant toutes les racines de $f(X)$.

Théorème 3.26. *Soit $f(X) \in K[X]$ un polynôme constant. Alors il existe une extension L/K contenant toutes les racines de $f(X)$.*

Démonstration. Si $\deg(f(X)) = 1$ alors par la remarque 3.8 $f(X)$ est irréductible et $L = K$. Par récurrence, supposons que tout polynôme de degré $d < n$ vérifie le théorème. Soit $f(X) = up_1(X)\dots p_n(X)$ la décomposition en polynômes irréductibles de $f(X)$ dans $K[X]$. Par la proposition 3.24 il existe une extension L_1/K contenant une racine α de $p_1(X)$. Dans cette extension $p_1(X) = (X - \alpha)q_1(X)$ avec $q_1(X) \in L_1[X]$. Par récurrence, comme $g(X) = uq_1(X)p_2(X)\dots p_n(X) \in L_1[X]$ est de degré strictement inférieur à $f(X)$, il existe un corps contenant toutes les racines de $g(X)$ et donc toutes celles de $f(X)$. □

Parmi les éléments d'une extension L/K il y a des éléments qui sont racines d'un polynôme à coefficients dans K et d'autres pas.

Définition 3.13. Un élément $\alpha \in L$ est algébrique sur K s'il existe un polynôme $f(X) \in K[X]$ tel que $f(\alpha) = 0$. Sinon, on dit que α est transcendant sur K. Si tous les éléments de L/K sont algébriques, on dit que L est une extension algébrique de K.

Example 3.27. L'élément $\alpha = \sqrt{2} + \sqrt{5}$ est algébrique sur $\mathbb{Q}$ car

$$\alpha^4 - 14\alpha^2 + 9 = 0$$

donc α est racine du polynôme $f(X) = X^4 - 14X^2 + 9 \in \mathbb{Q}[X]$.

De manière générale lorsque l'on dit que π est transcendant, on sous-entend transcendant sur $\mathbb{Q}$. La preuve de sa transcendance est non triviale et peut être trouvée [22] (Théorème de Lindemann-Weierstrass) ou [16] (Appendice 1). D'autres exemples de nombres transcendants sur $\mathbb{Q}$ sont donnés par $e = 2.718\ldots$, les nombres de Liouville, la constante de Gelfond-Schneider $2^{\sqrt{2}}$ etc... Dans notre contexte, la transcendance d'un nombre dépend évidemment du corps de base. Par exemple, par construction e est algébrique sur le corps $\mathbb{Q}[e]$. Il est en général difficile de prouver la transcendance d'un nombre.

Définition 3.14. Soit L/K une extension et soit $\alpha \in L$ un élément algébrique sur K. Le polynôme minimal $m_\alpha^K(X) \in K[X]$ de α est le polynôme monique de plus petit degré tel que $m_\alpha^K(\alpha) = 0$.

Dans le contexte de la définition précédente, on a la propriété suivante.

Proposition 3.28. *Le polynôme minimal $m_\alpha^K(X) \in K[X]$ d'un élément algébrique $\alpha \in L$ est un polynôme irréductible sur K.*

Démonstration. Supposons que $m_\alpha^K(X)$ n'est pas irréductible. Alors, il existe deux polynômes non constants $f(X), g(X) \in K[X]$ tel que $m_\alpha^K(X) = f(X)g(X)$. Par conséquent $0 = m_\alpha^K(\alpha) = f(\alpha)g(\alpha)$ et comme L est un corps, il est intègre et $f(\alpha) = 0$ ou $g(\alpha) = 0$. Or $f(X)$ et $g(X)$ sont des polynômes de degré inférieur strictement au degré de $m_\alpha^K(X)$. Ceci contredit la minimalité du degré de $m_\alpha^K(X)$. □

Le fait que $m_\alpha^K(X)$ soit monique le rend unique. De plus, si $f(X) \in K[X]$ est un polynôme qui possède aussi α comme racine alors $m_\alpha^K(X)$ divise $f(X)$ dans $K[X]$ (la preuve est omise).

Soit L/K et soit $\alpha \in L$. Considérons à nouveau l'homomorphisme d'anneaux $\psi_\alpha : K[X] \to K[\alpha] : f(X) \mapsto f(\alpha)$ (pour $n = 1$) construit dans la proposition 3.21. Supposons que α soit transcendant sur K. Alors, par définition, il n'existe pas de polynôme non nul $f(X) \in K[X]$ tel que $f(\alpha) = 0$ et $\mathrm{Ker}(\psi_\alpha) = \{0\}$. En conséquence, $K[X] \cong K[\alpha]$ et en prolongeant l'isomorphisme au corps des fractions $K(X) \cong K(\alpha)$. Maintenant, si α est un élément algébrique sur K alors $\mathrm{Ker}(\psi_\alpha)$ est un idéal non nul de $K[X]$. Si $f(X)$ est un polynôme irréductible tel que $f(\alpha) = 0$ alors $\mathrm{Ker}(\psi_\alpha) = \langle f(X)\rangle$. Par le premier théorème d'isomorphisme des anneaux, on a $K[X]/\langle f(X)\rangle \cong K[\alpha]$.

Théorème 3.29. *Soit α un élément algébrique sur K et $m_\alpha^K(X) \in K[X]$ son polynôme minimal. Posons $n = deg(m_\alpha^K(X))$, alors*

1. $K(\alpha) = K[\alpha] = K(X)/\langle m_\alpha^K(X)\rangle$
2. *une base de $K(\alpha)$ sur K est donnée par* $1, \alpha, \ldots, \alpha^{n-1}$
3. $[K(\alpha) : K] = n$

Démonstration. Les idéaux de $K[X]$ sont définis à unité près. Si $\epsilon \in K^*$ alors $\langle \epsilon f(X)\rangle = \langle f(X)\rangle$ pour tout polynôme irréductible $f(X) \in K[X]$. En particulier, on peut choisir $\epsilon \in K^*$ tel que $\epsilon f(X)$ est monique. Par conséquent, par le

paragraphe précédent $K[X]/\langle f(X)\rangle \cong K[X]/\langle m_\alpha^K(X)\rangle \cong K[\alpha]$ est un corps et $K[\alpha] \cong K(\alpha)$ car $K(\alpha)$ est le corps des fractions de $K[\alpha]$. Maintenant $K[\alpha] = \{f(\alpha) \mid f(X) \in K[X]\}$ et par la division euclidienne $f(X) = g(X)m_\alpha^K(X)+r(X)$ avec $\deg(r(X)) < \deg(m_\alpha^K(X)) = n$, on a $f(\alpha) = r(\alpha) = \sum_{i=0}^{n-1} r_i\alpha^i$. Donc $1, \alpha, \ldots, \alpha^{n-1}$ est une base de $K[\alpha] = K(\alpha)$. Avec cette base on voit que $K(\alpha)$ est un espace vectoriel de dimension n sur K, donc $[K(\alpha) : K] = n$. □

Example 3.30. L'élément $\sqrt[3]{2}$ est algébrique sur $\mathbb{Q}$. Son polynôme minimal est $X^3 - 2$. Par conséquent $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}[\sqrt[3]{2}]$ et une base de cette extension est $1, \sqrt[3]{2}, \sqrt[3]{2}^2$. Dès lors

$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\},$$

et $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3 = \deg(X^3 - 2)$.

On termine cette section en montrant une propriété importante des extensions algébriques.

Proposition 3.31. *Si L/K est une extension finie alors L/K est une extension algébrique.*

Démonstration. Si L/K est une extension finie, L peut être vu comme un espace vectoriel de dimension finie sur K. Soit n sa dimension. Alors $n+1$ éléments de L sont linéairement dépendants. Soit $\alpha \in L$, il existe $k_1, \ldots, k_n \in K$ non tous nuls tel que

$$k_1 + k_2\alpha + \cdots + k_{n-1}\alpha^{n-1} + k_n\alpha^n = 0.$$

Dès lors, il existe un polynôme de $K[X]$ qui possède α comme racine et α est algébrique sur K. □

Remarque 3.32. La réciproque n'est pas vraie. En effet, on peut montrer que

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \ldots, \sqrt{p}, \ldots),$$

où p parcourt l'ensemble des nombres premiers est une extension algébrique de $\mathbb{Q}$ mais qu'elle n'est pas finie.

Proposition 3.33. *Soit $\alpha_1, \ldots, \alpha_n$ un nombre fini d'éléments algébriques sur K. Alors $K(\alpha_1, \ldots, \alpha_n)$ est une extension finie.*

Démonstration. Si $n = 1$ alors $L_1 = K(\alpha_1)$ est une extension finie de K par le théorème 3.29. Par récurrence, supposons que $L_{n-1} = K(\alpha_1, \ldots, \alpha_{n-1})$ est une extension finie de K. Alors $L_n = K(\alpha_1, \ldots, \alpha_n)$ est une extension finie de L_{n-1} à nouveau par le théorème 3.29. Par le théorème 3.23 on sait que

$$[L_n : K] = [L_n : L_{n-1}][L_{n-1} : K] < +\infty$$

donc L_n/K est une extension finie. □

Proposition 3.34. *Si L/K et F/L sont des extensions algébriques alors F/K est une extension algbébrique.*

Démonstration. Soit $\alpha \in F$ et $m_\alpha^L(X) = \sum_{i=0}^n a_i X^i \in L[X]$ son polynôme minimal sur L. Alors $K(a_1, \ldots, a_n)/K$ est une extension finie par la proposition 3.33. Mais α est algébrique sur $K(a_1, \ldots, a_n)$ par conséquent $K(a_1, \ldots, a_n, \alpha)/K$ est finie à nouveau par 3.33 et donc algébrique par la proposition 3.31. Comme $\alpha \in F$ est quelconque F/K est une extension algébrique. □

3.4 Corps de décomposition et clôture algébrique

Soit K un corps et $f(X) \in K[X]$ un polynôme non constant. Dans la section précédente nous avons montré qu'il existe une extension L/K qui possède toutes les racines de $f(X)$.

Définition 3.15. Un polynôme $f(X) \in K[X]$ est dit scindé dans une extension L/K si

$$f(X) = a(X - \alpha_1)(X - \alpha_2) \ldots (X - \alpha_n) \in L[X],$$

où les α_i ne sont pas nécessairement distincts.

Autrement dit, un polynôme est scindé s'il peut s'écrire comme un produit de polynômes de degré 1 dans $L[X]$. Ou encore, le polynôme $f(X)$ est scindé dans L si toutes ses racines sont contenues dans L.

Définition 3.16. Le corps de décomposition d'un polynôme $f(X) \in K[X]$ est la plus petite extension L/K au sens de l'inclusion contenant toutes les racines de $f(X)$. Similairement c'est la plus petite extension dans laquelle $f(X)$ est scindé.

Clairement si $\alpha_1, \ldots, \alpha_n$ sont les racines de $f(X)$ alors $K(\alpha_1, \ldots, \alpha_n)$ est un corps de décomposition pour $f(X)$.

On montre que cette extension est unique à isomorphisme près. Cette partie fait intervenir des lemmes quelque peu techniques mais qui sont importants pour démontrer le théorème fondamental de la théorie de Galois.

Nous allons parler de prolongement d'homomorphisme de corps. Par le théorème 3.29 nous savons que les extensions peuvent se construire grâce à des quotients de la forme $F(\alpha) = F[X]/\langle f(X) \rangle$. Nous montrons d'abord qu'il est possible de prolonger un homomorphisme de corps à un homomorphisme sur les anneaux des polynômes.

Lemme 3.35. *Un homomorphisme de corps $\sigma : K \longrightarrow L$ peut-être prolongé à un homomorphisme d'anneaux $\sigma^* : K[X] \longrightarrow L[X]$ par*

$$\sigma^*(f(X)) = \sigma^*\left(\sum_{i=0}^n f_i X^i\right) = \sum_{i=0}^n \sigma(f_i) X^i.$$

Démonstration. En effet, pour tout $f(X), g(X) \in K[X]$ avec $f(X) = \sum_{i=0}^n a_i X^i$

et $g(X) = \sum_{i=0}^{m} b_i X^i$ on a

$$\begin{aligned}\sigma^*(f(X)+g(X)) &= \sigma^*\left(\sum_{i=0}^{n} a_i X^i + \sum_{i=0}^{m} b_i X^i\right)\\ &= \sum_{i=0}^{n} \sigma(a_i) X^i + \sum_{i=0}^{m} \sigma(b_i) X^i\\ &= \sigma^*(f(X)) + \sigma^*(g(X)),\end{aligned}$$

de plus, en posant $h(X) = \sum_{i=0}^{k} c_i X^i = f(X)g(X)$,

$$\begin{aligned}\sigma^*(f(X)g(X)) &= \sigma^*\left(\sum_{i=0}^{k} c_i X^i\right)\\ &= \sigma^*\left(\sum_{i=0}^{k} (a_0 b_i + a_1 b_{i-1} + \cdots + a_i b_0) X^i\right)\\ &= \sum_{i=0}^{k} \sigma(a_0 b_i + a_1 b_{i-1} + \cdots + a_i b_0) X^i\\ &= \sum_{i=0}^{k} (\sigma(a_0)\sigma(b_i) + \sigma(a_1)\sigma(b_{i-1}) + \cdots + \sigma(a_i)\sigma(b_0)) X^i\\ &= \sigma^*(f(X))\sigma^*(g(X)).\end{aligned}$$

Finalement, $\sigma^*(1X^0) = \sigma(1)X^0 = 1X^0$ donc σ^* est bien un homomorphisme d'anneaux. □

Il est clair que si σ est un isomorphisme alors σ^* aussi. Dans ce cas, si $f(X)$ est irréductible dans $K[X]$ alors $\sigma^*(f(X))$ est irréductible dans $L[X]$ et $\sigma^*(\langle f(X)\rangle) = \langle \sigma^*(f(X))\rangle$ est donc encore maximal dans $L[X]$.

Lemme 3.36. *Soit $\sigma : K_1 \to K_2$ un isomorphisme de corps. Soit $f(X) \in K_1[X]$ un polynôme irréductible et soit α une racine de $f(X)$ dans une extension L_1/K_1. Soit $\sigma^*(f(X)) \in K_2[X]$ de racine β dans l'extension L_2/K_2. Alors il existe un unique isomorphisme τ prolongeant σ tel que $\tau : K_1(\alpha) \to K_2(\beta)$ et $\tau(\alpha) = \beta$ avec $\tau|_{K_1} = \sigma$.*

Démonstration. Par le lemme précédent, σ se prolonge de manière unique en un isomorphisme d'anneaux $\sigma^* : K_1[X] \to K_2[X]$. Maintenant σ^* induit un isomorphisme $\psi : K_1[X]/\langle f(X)\rangle \to K_2[X]/\langle \sigma^*(f(X))\rangle$ et par le théorème 3.29 on sait qu'il existe des isomorphismes $\phi_1 : K_1(\alpha) \to K_1[X]/\langle f(X)\rangle$ et $\phi_2 : K_2(\beta) \to K_2[X]/\langle \sigma^*(f(X))\rangle$. Dès lors, il résulte que

$$K_1(\alpha) \xrightarrow{\phi_1} K_1[X]/\langle f(X)\rangle \xrightarrow{\psi} K_2[X]/\langle \sigma^*(f(X))\rangle \xrightarrow{\phi_2^{-1}} K_2(\beta)$$

où $\phi_1(\alpha) = x + \langle f(X)\rangle$ avec $\psi(x + \langle f(X)\rangle) = x + \langle \sigma^*(f(X))\rangle$ et $\phi_2^{-1}(x + \langle \sigma^*(f(X))) = \beta$ mais aussi $\phi_1(a) = a + \langle f(X)\rangle$ puis $\psi(a + \langle f(X)\rangle) = \sigma(a) +$

$\langle\sigma^*(f(X))\rangle$ et $\phi_2^{-1}(\sigma(a)+\langle\sigma^*(f(X))) = \sigma(a)$ pour tout $a \in K_1$. Par conséquent $\tau := \phi_2^{-1}\psi\phi_1$ est l'unique isomorphisme prolongeant σ et tel que $\tau(\alpha) = \beta$. □

Lemme 3.37. *Soit $\sigma : K_1 \to K_2$ un isomorphisme de corps et soit $\sigma^* : K_1[X] \to K_2[X]$ l'isomorphisme d'anneaux qui prolonge σ. Soit $f(X) \in K_1[X]$ dont le corps est décomposition est L_1 et soit $\sigma^*(f(X)) \in K[X]$ dont le corps de décomposition est L_2. Alors il existe un isomorphisme $\varphi : L_1 \to L_2$ prolongeant σ, c'est-à-dire tel que $\varphi|_{K_1} = \sigma$.*

Démonstration. On suit [26] (lemme 50). Si $f(X) \in K_1[X]$ est scindé dans $K_1[X]$ alors $\sigma^*(f(X))$ est scindé dans $K_2[X]$. Le corps de décomposition de $f(X)$ est K_1 et celui de $\sigma^*(f(X))$ est K_2, donc $\varphi = \sigma$. On procède par récurrence sur le degré du corps de décomposition. Si $[L_1 : K_1] \geq 2$ alors $f(X)$ possède un facteur irréductible $p(X)$ de degré ≥ 2 et de même $\sigma^*(f(X))$ possède le facteur irréductible $\sigma^*(p(X))$ de degré ≥ 2. Soit α une des racines de $p(X)$ et notons β une des racines de $\sigma^*(f(X))$. Alors par le lemme 3.36, il existe un unique isomorphisme $\tau : K_1(\alpha) \to K_2(\beta)$ qui prolonge σ avec $\tau(\alpha) = \beta$. Maintenant L_1 est toujours un corps de décomposition de $f(X)$ sur $K_1(\alpha)[X]$ et L_2 est toujours un corps de décomposition de $\sigma^*(f(X))$ sur $K_2(\beta)[X]$. Mais comme $[L_1 : K_1(\alpha)] < [L_1 : K_1]$, par l'hypothèse de récurrence il existe un isomorphisme $\tau' : L_1 \to L_2$ qui prolonge τ. □

Théorème 3.38. *(Unicité du corps de décomposition) Le corps de décomposition d'un polynôme est unique à isomorphisme près.*

Démonstration. On applique le théorème précédent pour $K_1 = K_2$ et $\sigma = \mathrm{id}$. Dès lors les corps de décomposition sont isomorphes. □

Par conséquent, tout polynôme non constant $f(X) \in K[X]$ possède un corps de décomposition et ce dernier est unique à isomorphisme près.

Définition 3.17. Un corps K est dit algébriquement clos s'il possède toutes les racines de tous les polynômes non constants à coefficients dans K.

Typiquement, $\mathbb{Q}$ et $\mathbb{R}$ ne sont pas algébriquement clos. Dans le premier cas $\mathbb{Q}$ ne contient pas les racines de X^2-2. Dans le second cas, $\mathbb{R}$ ne contient pas les racines de X^2+1. Cependant, le corps $\mathbb{C}$ est algébriquement clos. C'est le résultat du théorème fondamental de l'algèbre. De ce point de vue, il est très utile pour résoudre n'importe quelle équation polynomiale à coefficients dans $\mathbb{C}$ puisque les solutions de cette équations seront encore dans $\mathbb{C}$. Du point de vue de la théorie de Galois, ce corps est pauvre. En effet, il ne possède aucune extension algébrique non triviale (quels éléments pourrait-on lui adjoindre puisqu'il les contient déjà tous ? En fait on pourrait par exemple lui adjoindre une variable t pour obtenir le corps $\mathbb{C}(t)$ des fonctions rationnelles à coefficients dans $\mathbb{C}$ mais cette extension n'est pas algébrique). Il existe d'autres corps algébriquement clos.

Définition 3.18. La clôture algébrique d'un corps K est une extension algébrique $\overline{K}/K$ qui est algébriquement close.

De manière générale, on peut montrer (par le lemme de Zorn entre autres) que tout corps admet (à isomorphisme près) une unique clôture algébrique. Par conséquent, même si cela peut paraître assez abstrait, chaque corps fini $\mathbb{F}_p$ possède aussi une clôture algébrique notée $\overline{\mathbb{F}}_p$.

L'exemple classique est la clôture algébrique de $\mathbb{Q}$, notée $\overline{\mathbb{Q}}$. En particulier, $\overline{\mathbb{Q}}$ contient toutes les racines de tous les polynômes non constants à coefficients dans $\mathbb{Q}$. C'est la plus grande extension algébrique de $\mathbb{Q}$ et contrairement à $\mathbb{C}$, le corps $\overline{\mathbb{Q}}$ ne contient aucun élément transcendant sur $\mathbb{Q}$. Donc par exemple $\pi \notin \overline{\mathbb{Q}}$. Toute extension algébrique de $\mathbb{Q}$ peut être vue comme un sous-corps de $\overline{\mathbb{Q}}$.

3.5 Le groupe de Galois

Cette section s'inspire en particulier de [22] et [37]. La résolubilité des polynômes par radicaux est intimement liée à la structure d'un groupe associé à ce polynôme qu'on appelle groupe de Galois. Ce groupe est au coeur du théorème fondamental de la théorie de Galois. Pour pouvoir définir ce groupe, il nous faut définir les K-homomorphismes.

Définition 3.19. Soient F/K et L/K deux extensions de K et $\sigma : F \to L$ un homomorphisme de corps. On dit que σ est un K-homomorphisme si $\sigma(x) = x$ pour tout $x \in K$.

Rappelons qu'un automorphisme de corps est un isomorphisme d'un corps dans lui-même. On dit que l'automorphisme $\sigma : L \to L$ est un K-automorphisme si $\sigma(x) = x$ pour tout $x \in K$.

Définition 3.20. L'ensemble des K-automorphismes de L forme un groupe appelé groupe de Galois. Il est noté [2]

$$\mathrm{Gal}(L/K) = \{\sigma : L \to L \mid \text{où } \sigma \in \mathrm{Aut}(L) \text{ et } \sigma|_K = id\}$$

où Aut(L) désigne l'ensemble des automorphismes de L.

L'ensemble $\mathrm{Gal}(L/K)$ forme un groupe pour la composition.

Example 3.39. L'extension $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ est formée des éléments

$$\mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}.$$

Par définition, un élément de $\sigma \in$Gal$(\mathbb{Q}(\sqrt{5})/\mathbb{Q})$ doit vérifier $\sigma(a) = a$ pour tout $a \in \mathbb{Q}$. De ce fait $\sigma(a + b\sqrt{5}) = \sigma(a) + \sigma(b)\sigma(\sqrt{5}) = a + b\sigma(\sqrt{5})$. Maintenant comme $\sigma(\sqrt{5})\sigma(\sqrt{5}) = \sigma(\sqrt{5})^2 = \sigma(5) = 5$ on sait que $\sigma(\sqrt{5}) = \sqrt{5}$ ou $\sigma(\sqrt{5}) = -\sqrt{5}$. Si $\sigma(\sqrt{5}) = \sqrt{5}$ alors $\sigma(a + b\sqrt{5}) = a + b\sqrt{5}$ et $\sigma = id$. Si $\sigma(\sqrt{5}) = -\sqrt{5}$ alors $\sigma(a + b\sqrt{5}) = a - b\sqrt{5}$. Par conséquent, le groupe de Galois de $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ est $\mathrm{Gal}(\mathbb{Q}(\sqrt{5})/\mathbb{Q}) = \{id, \sigma\}$ et on vérifie tout de suite que $\sigma \circ \sigma = \sigma^2 = id$.

2. Certains auteurs préfèrent réserver la notation $\mathrm{Gal}(L/K)$ aux extensions galoisiennes et utilisent plutôt la notation $\mathrm{Aut}(L/K)$ pour désigner le groupe des automorphismes d'une extension quelconque. Nous ne pensons pas que cela créée de confusion.

La première grande propriété des éléments du groupe de Galois est qu'ils agissent sur les racines des polynômes à coefficients dans le corps de base.

Proposition 3.40. *Soit K un corps, $f(X) \in K[X]$ un polynôme non constant et L son corps de décomposition. Soit $\sigma \in Gal(L/K)$ et soit $\alpha \in L$ une racine de $f(X)$. Alors $\sigma(\alpha) \in L$ est encore une racine de $f(X)$.*

Démonstration. Soit $f(X) = \sum_{i=0}^{n} a_i X^i$ l'expression du polynôme en question. Alors

$$0 = \sigma(0) = \sigma(f(\alpha)) = \sigma\left(\sum_{i=0}^{n} a_i \alpha^i\right) = \sum_{i=0}^{n} a_i \sigma(\alpha)^i$$

et $f(\sigma(\alpha)) = 0$, d'où la conclusion. □

Dans l'exemple précédent, $\mathbb{Q}(\sqrt{5})$ est le corps de décomposition de $f(X) = X^2 - 5$. De plus $\mathrm{Gal}(\mathbb{Q}(\sqrt{5})/\mathbb{Q}) = \{id, \sigma\}$ avec $\sigma(\sqrt{5}) = -\sqrt{5}$. Or $\sqrt{5}$ et $-\sqrt{5}$ sont les racines de $X^2 - 5$ et on voit bien que le groupe de Galois agit sur les racines de $f(X)$.

Notons encore que dans l'exemple précédent, les éléments de $\mathrm{Gal}(\mathbb{Q}(\sqrt{5})/\mathbb{Q})$ sont entièrement déterminés par leur action sur $\sqrt{5}$. Plus généralement, on a le résultat suivant.

Proposition 3.41. *Soit $L = K(S)$ une extension de K générée par un sous-ensemble $S \subset L$. Alors les éléments de $Gal(L/K)$ sont entièrement déterminés par leur action sur S, i.e. $\sigma|_S = \tau|_S \implies \sigma = \tau$ pour tout $\sigma, \tau \in Gal(L/K)$.*

Démonstration. Cela se voit facilement en notant que si $\alpha \in L$ alors il existe des éléments $w_1, \ldots, w_n \in S$ tels que $\alpha \in K(w_1, \ldots, w_n)$. Par le corollaire 3.22 nous savons alors qu'il existe $f, g \in K[X_1, \ldots, X_n]$ tels que

$$\alpha = \frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)}.$$

Donc, si σ_1, σ_2 sont deux automorphismes de $\mathrm{Gal}(L/K)$ alors

$$\sigma_i(\alpha) = \frac{f(\sigma_i(\alpha_1), \ldots, \sigma_i(\alpha_n))}{g(\sigma_i(\alpha_1), \ldots, \sigma_i(\alpha_n))},$$

pour $i = 1, 2$ puisque f, g sont à coefficients dans K. Par conséquent, si on suppose que $\sigma_1|_S = \sigma_2|_S$, il vient en particulier que $\sigma_1(\alpha_i) = \sigma_1(\alpha_i)$ pour tout $i = 1, \ldots, n$ et donc que $\sigma_1(\alpha) = \sigma_2(\alpha)$. Comme α est arbitraire cela montre que $\sigma_1|_S = \sigma_2|_S \implies \sigma_1 = \sigma_2$. □

En particulier, si $K(\alpha)/K$ est une extension finie, alors les éléments de $\mathrm{Gal}(K(\alpha)/K)$ peuvent être déterminés en regardant leur action sur α et en prenant en compte que $\sigma(\alpha) = \beta$ où β est aussi une racine du polynôme minimal de α sur K.

Proposition 3.42. *Si L/K est une extension finie alors $|Gal(L/K)|$ est fini.*

Démonstration. Si L/K est finie alors il existe des éléments $\alpha_1, \ldots, \alpha_n \in L$ tels que $L = K(\alpha_1, \ldots, \alpha_n)$. Par la proposition précédente, deux éléments $\sigma, \tau \in \mathrm{Gal}(L/K)$ sont distincts si et seulement si il existe $1 \leq i \leq n$ tel que $\sigma(\alpha_i) \neq \tau(\alpha_i)$. Maintenant, chaque $C_i = \{\sigma(\alpha_i) \mid \sigma \in \mathrm{Gal}(L/K)\}$ est fini puisque les $\sigma(\alpha_i)$ correspondent aux racines du polynôme minimal $m_{\alpha_i}(X) \in K[X]$ de α_i. Donc $\mathrm{Gal}(L/K)$ est fini. □

Définition 3.21. Soit $S \subseteq \mathrm{Gal}(L/K)$. Le corps

$$\mathrm{Fix}(S) = \{x \in L \mid \sigma(x) = x \ , \forall \sigma \in S\},$$

est appelé le corps fixé par S.

Démonstration. On veut montrer que $F = \mathrm{Fix}(S)$ est bien un corps. On sait que $K \subseteq F$ par définition du groupe de Galois, par conséquent $0, 1 \in F$. Soient $x, y \in F$ et soit $\sigma \in S$. Par définition d'un automorphisme et comme $F = \mathrm{Fix}(S)$, $\sigma(x + y) = \sigma(x) + \sigma(y) = x + y$ donc $x + y \in F$. Ensuite $\sigma(xy) = \sigma(x)\sigma(y) = xy$ donc $xy \in F$. Finalement si $x \neq 0$ alors $\sigma(x^{-1}) = \sigma(x)^{-1} = x^{-1} \in F$. Maintenant $F = \cap_{\sigma \in S}\mathrm{Fix}(\{\sigma\})$ et l'intersection de deux corps est encore un corps d'où la conclusion. □

À priori, si $K \subseteq E \subseteq L$ est un corps intermédiaire entre L et K alors $E \subseteq \mathrm{Fix}(\mathrm{Gal}(L/E))$ par la définition même de corps fixé.

Définition 3.22. Une extension L/K est galoisienne si $\mathrm{Fix}(\mathrm{Gal}(L/K)) = K$.

Example 3.43. L'extension $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ est galoisienne car les seuls éléments de $\mathbb{Q}(\sqrt{5})$ fixés par σ (et id) sont les éléments $a+b\sqrt{5} \in \mathbb{Q}(\sqrt{5})$ tels que $\sigma(a+b\sqrt{5}) = a - b\sqrt{5} = a + b\sqrt{5}$, c'est-à-dire ceux pour lesquels $b = 0$. Autrement dit, $\mathrm{Fix}(\mathrm{Gal}(\mathbb{Q}(\sqrt{5})/\mathbb{Q})) = \mathbb{Q}$.

Example 3.44. L'extension $\mathbb{Q}(\sqrt[3]{3})/\mathbb{Q}$ n'est pas galoisienne. En effet, $\sqrt[3]{3}$ est racine de $X^3 - 3$ dans $\mathbb{Q}$ et $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{3})/\mathbb{Q})$ envoie une racine de $X^3 - 3$ sur une autre de ses racines. Or les racines de $X^3 - 3$ dans son corps de décomposition sont $\sqrt[3]{3}$, $\sqrt[3]{3}e^{2i\pi/3}$ et $\sqrt[3]{3}e^{4i\pi/3}$. Par le théorème 3.29 nous savons que

$$\mathbb{Q}(\sqrt[3]{3}) = \{a + b\sqrt[3]{3} + c\sqrt[3]{3^2} \mid a, b, c \in \mathbb{Q}\},$$

et clairement, cet ensemble ne contient ni $e^{2i\pi/3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ ni $e^{2i\pi/3} = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$. En outre, σ est entièrement déterminé par son action sur $\sqrt[3]{3}$ et nous voyons donc que $\sigma(\sqrt[3]{3}) = \sqrt[3]{3}$, ou encore que $\sigma = \mathrm{id}$. Mais alors $\mathbb{Q} \subset \mathrm{Fix}(\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{3})/\mathbb{Q})) = \mathbb{Q}(\sqrt[3]{3})$, d'où l'assertion.

Si $K \subseteq E_1 \subseteq E_2 \subseteq L$ alors $\mathrm{Gal}(L/E_2) \subseteq \mathrm{Gal}(L/E_1)$ puisque si $\sigma \in \mathrm{Gal}(L/E_2)$ alors $\sigma(\alpha) = \alpha$ pour tout $\alpha \in E_2$ et donc, en particulier $\sigma(\alpha) = \alpha$ pour tout $\alpha \in E_1$. Si $S_1 \subseteq S_2$ sont deux sous-ensembles quelconques de $\mathrm{Gal}(L/K)$ alors $\mathrm{Fix}(S_2) \subseteq \mathrm{Fix}(S_1)$. Intuitivement, S_2 possède plus d'éléments que S_1, donc il y a plus de contraintes sur le corps fixé par S_2 et ce dernier est plus petit que le corps fixé par S_1. Cependant, il se peut que $\mathrm{Fix}(S_1) = \mathrm{Fix}(S_2)$

même si $S_1 \neq S_2$. On peut par exemple penser au cas $S_1 = \{\sigma\}$ et $S_2 = \{\sigma, \mathrm{id}\}$ où $\sigma \in \mathrm{Gal}(L/K)$. Notons $\mathcal{S}$ l'ensemble des parties [3] de $\mathrm{Gal}(L/K)$ et $\mathcal{F}$ l'ensemble des corps intermédiaires entre L et K. Soit

$$\Gamma : \mathcal{S} \to \mathcal{F} : S \mapsto \mathrm{Fix}(S),$$

la fonction qui associe à un sous-ensemble $S \subseteq \mathrm{Gal}(L/K)$ son corps fixé. Comme nous l'avons vu, cette fonction n'est pas injective et il n'est pas non plus dit qu'elle soit surjective. Notons aussi

$$\Omega : \mathrm{Im}(\Gamma) \to \mathcal{S} : E \mapsto \mathrm{Gal}(L/E).$$

Proposition 3.45. *Si $E \in Im(\Gamma)$ alors $E = Fix(Gal(L/E))$. Inversement, soit $S \in \mathcal{S}$. S'il existe $E \in Im(\Gamma)$ tel que $S = Gal(L/E)$ alors $S = Gal(L/Fix(S))$.*

Démonstration. Comme $E \in \mathrm{Im}(\Gamma)$ il existe $S \in \mathcal{S}$ tel que $E = \mathrm{Fix}(S)$. En outre, on a vu que $E \subseteq \mathrm{Fix}(\mathrm{Gal}(L/E))$. Maintenant on a $S \subseteq \mathrm{Gal}(L/\mathrm{Fix}(S))$. En effet, si $\sigma \in S$ alors $\sigma(\alpha) = \alpha$ pour tout $\alpha \in \mathrm{Fix}(S)$ et donc $\sigma \in \mathrm{Gal}(L/\mathrm{Fix}(S))$. Mais si $S \subseteq \mathrm{Gal}(L/\mathrm{Fix}(S))$ alors $\mathrm{Fix}(\mathrm{Gal}(L/\mathrm{Fix}(S))) \subseteq \mathrm{Fix}(S) = E$ donc $E = \mathrm{Fix}(\mathrm{Gal}(\mathrm{L}/\mathrm{Fix}(\mathrm{S}))) = \mathrm{Fix}(\mathrm{Gal}(\mathrm{L}/\mathrm{E}))$.

Inversement, soit $S = \mathrm{Gal}(L/E)$ où $E \in \mathrm{Im}(\Gamma)$. Par ce qui précède nous savons que $S \subseteq \mathrm{Gal}(L/\mathrm{Fix}(S))$. En outre $E \subseteq \mathrm{Fix}(S) = \mathrm{Fix}(\mathrm{Gal}(L/E))$. Donc $S = \mathrm{Gal}(L/E) \supseteq \mathrm{Gal}(K/\mathrm{Fix}(S))$, d'où $S = \mathrm{Gal}(L/\mathrm{Fix}(S))$. □

Cette proposition nous dit ceci : Si $E_1 \neq E_2$ sont deux corps intermédiaires de L/K dans l'image de Γ, alors $\mathrm{Fix}(\mathrm{Gal}(L/E_1)) = E_1 \neq E_2 = \mathrm{Fix}(\mathrm{Gal}(L/E_2))$ et $\mathrm{Gal}(L/E_1) \neq \mathrm{Gal}(L/E_2)$. En d'autres termes,

$$E_1 \neq E_2 \implies \Omega(E_1) \neq \Omega(E_2).$$

Inversement, la deuxième partie de la proposition nous dit que si $\mathrm{Gal}(L/E_1) = S_1 \neq S_2 = \mathrm{Gal}(L/E_1)$ alors $S_1 = \mathrm{Fix}(\mathrm{Gal}(L/\mathrm{Fix}(S_1))) \neq \mathrm{Fix}(\mathrm{Gal}(L/\mathrm{Fix}(S_2))) = S_2$, c'est-à-dire $\mathrm{Fix}(S_1) \neq \mathrm{Fix}(S_2)$. En d'autres termes,

$$\mathrm{Gal}(L/E_1) \neq \mathrm{Gal}(L/E_2) \implies \Gamma(S_1) \neq \Gamma(S_2).$$

Maintenant si $S_1 \neq S_2$ sont deux sous-ensembles quelconques de $\mathrm{Gal}(L/K)$ tels que $\mathrm{Fix}(S_1) = \mathrm{Fix}(S_2) = E$ alors il existe un unique sous-groupe $\mathrm{Gal}(L/E)$ tel que $\mathrm{Fix}(\mathrm{Gal}(L/E)) = \mathrm{Fix}(S_1) = \mathrm{Fix}(S_2) = E$. Autrement dit, si on restreint le domaine de la fonction Γ à l'ensemble des sous-groupes $\mathcal{G}$ de $\mathrm{Gal}(L/K)$ alors

$$\Gamma : \mathcal{G} \to \mathrm{Im}(\Gamma) : \mathrm{Gal}(L/E) \mapsto \mathrm{Fix}(\mathrm{Gal}(L/E)) = E$$

est une bijection et sa fonction inverse est Ω.

Example 3.46. Considérons l'extension $\mathbb{Q}(\sqrt[4]{5})/\mathbb{Q}$. Le polynôme minimal de $\sqrt[4]{5}$ est $f(X) = X^4 - 5$. On a donc $[\mathbb{Q}(\sqrt[4]{5}) : \mathbb{Q}] = 4$. Maintenant les racines

3. On exclu l'ensemble vide.

de $X^4 - 5$ dans son corps de décomposition sont $\alpha_1 = \sqrt[4]{5}, \alpha_2 = -\sqrt[4]{5}, \alpha_3 = i\sqrt[4]{5}, \alpha_4 = -i\sqrt[4]{5}$. Manifestement, α_1 et α_2 appartiennent à $\mathbb{Q}(\sqrt[4]{5})$ tandis que α_3 et α_4 pas. Un élément $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt[4]{5})/\mathbb{Q})$ dépend entièrement de son action sur $\sqrt[4]{5}$. Comme α_2 est la seule autre racine de $X^4 - 5$ dans $\mathbb{Q}(\sqrt[4]{5})$ on a soit $\sigma(\sqrt[4]{5}) = \sqrt[4]{5}$ soit $\sigma(\sqrt[4]{5}) = -\sqrt[4]{5}$. Par conséquent $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{5})/\mathbb{Q}) = \{\mathrm{id}, \sigma\} \cong \mathbb{Z}/2\mathbb{Z}$ où $\sigma^2 = \mathrm{id}$. Pourtant, il est clair que

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\sqrt[4]{5}).$$

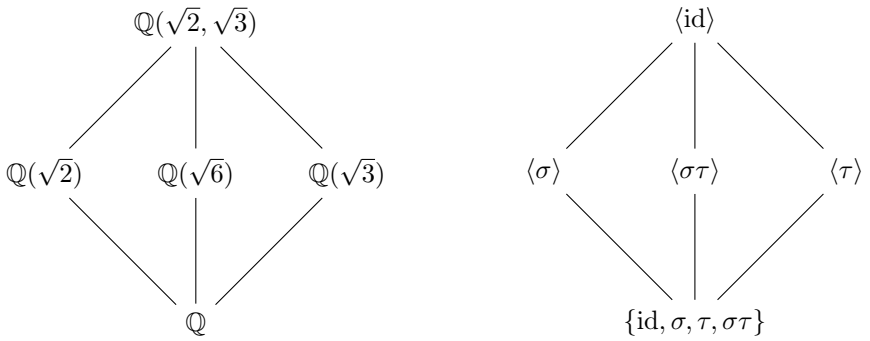
Dès lors, la correspondance est imparfaite : Il n'y a pas de bijection entre l'ensemble des corps intermédiaire de $\mathbb{Q}$ et $\mathbb{Q}(\sqrt[4]{5})$ et l'ensemble des sous-groupes de $\mathbb{Z}/2\mathbb{Z}$. En outre,

$$\sigma(\sqrt{5}) = \sigma(\sqrt[4]{5}^2) = \sigma(\sqrt[4]{5})^2 = (-\sqrt[4]{5})^2 = \sqrt{5}$$

donc $\mathbb{Q} \subset \mathrm{Fix}(\mathbb{Z}/2\mathbb{Z}) = \mathbb{Q}(\sqrt{5})$, d'où le diagramme suivant.

$$\begin{array}{ccc} \mathbb{Q}(\sqrt[4]{5}) & & \langle \mathrm{id} \rangle \\ \Big| 2 & & \Big| \\ \mathbb{Q}(\sqrt{5}) & & \mathbb{Z}/2\mathbb{Z} \\ \Big| 2 & & \Big| \\ \mathbb{Q} & & \mathbb{Z}/2\mathbb{Z} \end{array}$$

Example 3.47. Considérons l'extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$. Cette extension est de degré 4 sur $\mathbb{Q}$ par l'exemple 3.20. On se convainc facilement que $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \{\mathrm{id}, \sigma, \tau, \sigma\tau\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ où $\sigma(\sqrt{2}) = \sqrt{2}, \sigma(\sqrt{3}) = -\sqrt{3}$ et $\tau(\sqrt{2}) = -\sqrt{2}, \tau(\sqrt{3}) = \sqrt{3}$. Les sous-groupes de $\{\mathrm{id}, \sigma, \tau, \sigma\tau\}$ sont $\langle \mathrm{id} \rangle$, $\langle \sigma \rangle$, $\langle \tau \rangle$ et $\langle \sigma\tau \rangle$. Dans le même temps, les corps intermédiaires de $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ sont $\mathbb{Q} = \mathrm{Fix}(\mathbb{Z}/2\mathbb{Z})$, $\mathbb{Q}(\sqrt{2}) = \mathrm{Fix}(\langle \sigma \rangle)$, $\mathbb{Q}(\sqrt{3}) = \mathrm{Fix}(\langle \tau \rangle)$ et il ne faut pas oublier $\mathbb{Q}(\sqrt{6}) = \mathrm{Fix}(\langle \sigma\tau \rangle)$. On peut montrer qu'il n'y a pas d'autres corps intermédiaires et on a donc une bijection entre l'ensemble des corps intermédiaire de $\mathbb{Q}$ et $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ et l'ensemble des sous-groupes de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Le diagramme suivant illustre la correspondance.



Autant le dire tout de suite, la correspondance de l'exemple 3.46 n'est pas une bijection car $\mathbb{Q} \subset \mathrm{Fix}(\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{5})/\mathbb{Q}))$ et non pas $\mathbb{Q} = \mathrm{Fix}(\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{5})/\mathbb{Q}))$. Pour le redire, au vu de la définition d'une extension galoisienne, la correspondance de l'exemple 3.46 n'est pas une bijection car $\mathbb{Q}(\sqrt[4]{5})/\mathbb{Q}$ n'est pas galoisienne. Inversement, la correspondance de l'exercice 3.47 est une bijection car $\mathbb{Q} = \mathrm{Fix}(\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}))$, c'est-à-dire, parce que $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ est une extension galoisienne. Si le lecteur ne voit pas pourquoi, c'est simplement parce que nous ne l'avons pas encore démontré. Sans surprise, cette histoire de correspondance est l'objet du théorème fondamental de la théorie de Galois.

Les prochaines démonstrations sont en quelques sorte inévitables et se retrouvent dans tous les ouvrages de la théorie de Galois.

Définition 3.23. Soit G un groupe et soit $K^\times$ le groupe multiplicatif des unités d'un corps K. Un caractère de G dans K est un homomorphisme $\sigma : G \to K^\times$.

Définition 3.24. Un ensemble de caractères $\{\sigma_1, \ldots, \sigma_n\}$ de G dans K est dépendant s'il existe $\alpha_1, \ldots, \alpha_n \in K^\times$ tel que pour tout $a \in G$ on a

$$\sum_{i=1}^{n} \alpha_i \sigma_i(a) = 0.$$

S'il n'existe pas de tels a_i on dira que les caractères $\{\sigma_1, \ldots, \sigma_n\}$ sont indépendants.

Nous suivons la démonstration du lemme 2.12 de [22]. (Sinon nous pouvons suivre la démonstration par récurrence de Artin présentée dans la preuve du théorème 2.8.4 de [37] ou encore par lemme 76 de [26].)

Lemme 3.48. *(Lemme de Dedekind) Soient $\{\sigma_1, \ldots, \sigma_n\}$ des caractères distincts de G dans K. Alors ces caractères sont indépendants.*

Démonstration. Supposons par l'absurde que ces caractères sont dépendants. Alors il existe des éléments $\alpha_1, \ldots, \alpha_n \in K$ non tous nuls tel que

$$\sum_{i=1}^{n} \alpha_i \sigma_i(a) = 0,$$

pour tout $a \in G$. Soit m le plus petit indice tel que (en permutant les indices si nécessaire) les caractères $\sigma_1, \ldots, \sigma_m$ sont encore dépendants sur K et notons à nouveau $\alpha_1, \ldots, \alpha_m \in K$ les coefficients de la combinaison linéaire telle que $\sum_{i=1}^{m} \alpha_i \sigma_i(a) = 0$ pour tout $a \in G$. Comme $\sigma_i \neq \sigma_j$ pour tout $i \neq j$, il existe $b \in G$ tel que $\sigma_1(b) \neq \sigma_2(b)$. Dès lors

$$\sum_{i=1}^{m} \alpha_i \sigma_i(a)\sigma_1(b) = 0,$$

et

$$\sum_{i=1}^{m} \alpha_i \sigma_i(ab) = \sum_{i=1}^{m} \alpha_i \sigma_i(a)\sigma_i(b) = 0,$$

pour tout $a \in G$. En soustrayant la première à la deuxième on obtient

$$\sum_{i=1}^{m} (\alpha_i \sigma_i(a)\sigma_i(b) - \alpha_i \sigma_i(a)\sigma_1(b)) = \sum_{i=2}^{m} (\sigma_i(b) - \sigma_1(b))\alpha_i \sigma_i(a) = 0,$$

qui est une combinaison linéaire de $m-1$ caractères qui s'annule. Ceci contredit la minimalité de m. Donc les caractères sont indépendants. □

Les caractères qui nous intéressent sont ceux où $G = K^\times$ est le groupe multiplicatif des unités d'un corps K, c'est-à-dire, les homomorphismes $\sigma : L^\times \to L^\times$.

Lemme 3.49. *Si $S \subseteq Gal(L/K)$ alors $|S| \leq [L : Fix(S)]$.*

Démonstration. On suit [37] et [26]. Supposons dans un premier temps que $r = [L : K] < n = \mathrm{Card}(S)$. Soient $w_1, \ldots, w_r$ des éléments de L formant une base du K-espace vectoriel L. Soit le système de r équations à n inconnues,

$$\begin{aligned} x_1\sigma_1(w_1) + \cdots + x_n\sigma_n(w_1) &= 0 \\ x_1\sigma_1(w_2) + \cdots + x_n\sigma_n(w_2) &= 0 \\ \vdots \qquad\qquad\qquad \vdots \qquad &\vdots \\ x_1\sigma_1(w_r) + \cdots + x_n\sigma_n(w_r) &= 0. \end{aligned} \tag{1}$$

Comme $r < n$, il existe une infinité de solutions à ce système et en particulier il existe une solution de la forme $[\alpha_1, \ldots, \alpha_n]$ où les $a_i \in L$ ne sont pas tous nuls. Soit $\beta \in L$. Il existe alors des coefficients $\beta_1, \ldots, \beta_r \in K$ tel que $\beta = \sum_{i=1}^{r} \beta_i w_i$. Alors

$$\begin{aligned} \sum_{i=1}^{n} \alpha_i \sigma_i(\beta) &= \sum_{i=1}^{r} \alpha_i \sigma_i \left(\sum_{j=1}^{r} \beta_i w_i \right) \\ &= \sum_{i=1}^{n} \sum_{j=1}^{r} \alpha_i \beta_j \sigma(w_j), \text{ car } \sigma \in \mathrm{Gal}(L/K) \\ &= \sum_{j=1}^{r} \beta_j \left(\sum_{i=1}^{n} \alpha_i \sigma(w_j) \right) \\ &= 0 \end{aligned}$$

car $[\alpha_1, \ldots, \alpha_n]$ est une solution de l'équation (1). Mais alors $\sum_{i=1}^{n} \alpha_i \sigma_i(\beta) = 0$ où β était arbitrairement choisi dans L, donc les σ_i sont linéairement dépendants, ce qui est impossible par le lemme de Dedekind 3.48. □

Corollaire 3.50. *Soit L/K une extension finie et posons $n = [L : K]$. Alors tout élément $\alpha \in L$ a au plus n conjugués distincts dans L.*

Démonstration. Soit $\alpha \in L$. On sait que $[L : K] = n \geq |\mathrm{Gal}(L/K)|$ par le lemme précédent. Par conséquent l'ensemble $\{\sigma(\alpha) \mid \sigma \in \mathrm{Gal}(L/K)\}$ a au plus n éléments distincts. □

Lemme 3.51. *Si $S = Gal(L/E)$ pour un certain $K \subset E \subset L$ alors $Card(S) = [L : Fix(S)]$.*

Démonstration. Soit n le cardinal de S et $r = [L : \mathrm{Fix}(S)]$. Supposons que $r > n$. Dès lors il existe au moins $n+1$ éléments de L linéairement indépendants sur K. Soient $w, \ldots, w_{n+1} \in E$ de tels éléments. Considérons le systèmes d'équations de n équations à $n+1$ inconnues

$$\begin{aligned} x_1\sigma_1(w_1) + \cdots + x_{n+1}\sigma_1(w_{n+1}) &= 0 \\ x_1\sigma_2(w_1) + \cdots + x_{n+1}\sigma_2(w_{n+1}) &= 0 \\ \vdots \qquad\qquad\qquad \vdots \qquad &\vdots \\ x_1\sigma_n(w_1) + \cdots + x_{n+1}\sigma_r(w_{n+1}) &= 0. \end{aligned} \tag{2}$$

Ce système possède une solution non triviale puisqu'il y a plus d'inconnues que d'équations. Soit $[\alpha_1, \ldots, \alpha_{n+1}]$ une telle solution. Supposons en plus que cette solution est choisie de sorte qu'il y a un nombre minimal de $\alpha_i \neq 0$. Quitte à permuter les indices, on peut suppose que $\alpha_i \neq 0$ pour $i = 1, \ldots, s$ et $\alpha_j = 0$ pour $s < j \leq n+1$. On a $s > 1$. En effet, S est un groupe, donc $\mathrm{id} \in S$ et sans perte de généralité on peut supposer que $\sigma_1 = \mathrm{id}$. En outre, si $s = 1$ alors $\alpha_1\sigma_1(w_1) = \alpha_1 w_1 = 0$ et comme $w_1 \neq 0$ on a $\alpha_1 = 0$, ce qui contredit $s = 1$. On peut ensuite supposer que la solution est de la forme $[\alpha_1, \ldots, \alpha_{s-1}, 1, 0, \ldots, 0]$ en multipliant les α_i par α_s^{-1} si nécessaire. Il existe au moins un des $\alpha_i \notin K$ car sinon $0 = \alpha_1\sigma_1(w_1) + \cdots + \alpha_s\sigma_1(w_s) = \alpha_1 w_1 + \cdots + \alpha_s w_s = 0$ et les $w_1, \ldots, w_n$ ne seraient pas linéairement indépendants. En permutant encore les α_i on peut supposer que $\alpha_1 \notin K$. Après toutes ces déductions on a que

$$\alpha_1\sigma_i(w_1) + \cdots + \alpha_s\sigma_i(w_s) = 0 \tag{3}$$

pour tout $1 \leq i \leq r$. En appliquant σ_k à cette équation pour chaque $\sigma_k \in S$ on a

$$\sigma_k(\alpha_1)\sigma_k(\sigma_i(w_1)) + \cdots + \sigma_k(\alpha_s)\sigma_k(\sigma_i(w_s)) = 0$$

et comme S est un groupe il existe pour chacun des σ_k un $\sigma_j \in S$ tel que $\sigma_j = \sigma_k\sigma_i$ de sorte que

$$\sigma_k(\alpha_1)\sigma_j(w_1) + \cdots + \sigma_k(\alpha_s)\sigma_j(w_s) = 0. \tag{4}$$

En soustrayant les équations (3) pour $i = j$ aux équations (4) on a

$$(\sigma_k(\alpha_1) - \alpha_1)\sigma_j(w_1) + \cdots + (\sigma_k(\alpha_{s-1}) - \alpha_{s-1})\sigma_j(w_{s-1}) = 0,$$

pour $1 \leq j \leq n$. Comme $\sigma_k(\alpha_1) - \alpha_1 \neq 0$ on a une solution à (2) avec moins de s éléments non nuls, ce qui contredit la minimalité de s. □

Corollaire 3.52. *L'extension L/K est galoisienne si et seulement si $[L : K] = |Gal(L/K)|$.*

Démonstration. Si L/K est galoisienne alors $\mathrm{Fix}(\mathrm{Gal}(L/K)) = K$, donc $[L : K] = |\mathrm{Gal}(L/K)|$ par le lemme précédent. Inversement, supposons que $[L : K] = |\mathrm{Gal}(L/K)|$. Par définition $K \subseteq \mathrm{Fix}(\mathrm{Gal}(L/K))$. Maintenant posons $E = \mathrm{Fix}(\mathrm{Gal}(L/K))$. On a aussi $E = \mathrm{Fix}(\mathrm{Gal}(L/E))$ et comme $\mathrm{Gal}(L/K)$ et $\mathrm{Gal}(L/E)$ sont des groupes, on sait que cela implique que $\mathrm{Gal}(L/K) = \mathrm{Gal}(L/E)$. Mais alors

$$[L : E] \geq |\mathrm{Gal}(L/E)| = |\mathrm{Gal}(L/K)| = [L : K],$$

et comme $K \subseteq E \subseteq L$ cela montre que $[L : K] = [L : E]$. Par conséquent $E = K$ et $K = \mathrm{Fix}(\mathrm{Gal}(L/K))$ et l'extension est galoisienne. □

3.6 Extensions normales et extensions séparables

Définition 3.25. Une extension algébrique L/K est dite normale si le polynôme minimal de tout élément de L est scindé dans L.

En d'autres termes une extension est normale si le polynôme minimal de tout élément de L possède toutes ses racines dans L. Il ne faut pas aller chercher loin pour trouver une telle extension. On peut, par exemple, penser à l'extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$.

Si l'extension L/K n'est pas normale, alors il existe une plus petite extension E/L telle que E/K est normale. On appelle cette extension la **clôture normale** de L/K.

Définition 3.26. Soit $f(X) \in K[X]$ un polynôme non constant. L'ordre d'une racine α est le plus grand entier positif n tel que $(X - \alpha)^n$ divise $f(X)$. Si $n = 1$ on dit que α est une racine simple de $f(X)$. Si $n > 1$, on dit que α est une racine multiple.

Proposition 3.53. *Soit $K \subseteq E \subseteq L$ une tour d'extensions. Si L/K est une extension normale alors L/E l'est aussi.*

Démonstration. Soit $\alpha \in L$ et soit $m_\alpha(X) \in K$ son polynôme minimal. Par hypothèse toutes les racines de $m_\alpha(X)$ sont dans L. Or, le polynôme minimal de α sur E est un facteur de $m_\alpha(X)$, donc toutes ses racines sont encore dans L. Par conséquent L/E est une extension normale. □

Définition 3.27. Si $f(X)$ admet la factorisation en polynômes irréductibles

$$f(X) = p_1(X) \dots p_1(X) \in K[X],$$

alors on dit que $f(X)$ est séparable si chacun des $p_i(X)$ ne possède que des racines simples [4].

Définition 3.28. Une extension algébrique L/K est dite séparable si le polynôme minimal de tout élément est séparable.

Proposition 3.54. *Soit $K \subseteq E \subseteq L$ une tour d'extensions. Si L/K est une extension séparable alors L/E l'est aussi.*

Démonstration. Soit $\alpha \in L$ et soit $m_\alpha(X)$ son polynôme minimal sur K. Par hypothèse $m_\alpha(X)$ ne possède que des racines simples. Maintenant, le polynôme minimal de $f(X)$ de α sur E est un facteur de $m_\alpha(X)$. Par conséquent, toutes les racines de $f(X)$ sont simples et cela montre que L/E est une extension séparable. □

Il y a un critère qui permet de savoir si un polynôme irréductible est séparable ou non.

Définition 3.29. Soit $f(X) = \sum_{i=0}^{n} a_i X^i \in K[X]$ non nul. Le polynôme dérivé de $f(X)$ est $f'(X) = \sum_{i=0}^{n} i a_i X^{i-1}$.

Avec cette définition, il est clair que cette dérivation formelle vérifie toutes les propriétés de la dérivation classique (règle de Leibniz etc...).

Proposition 3.55. *Soit $f(X) \in K[X]$ un polynôme non constant. Soit L le corps de décomposition de $f(X)$ et $\alpha \in L$ une racine de $f(X)$. Alors α est une racine simple de $f(X)$ si et seulement si $f'(\alpha) \neq 0$.*

Démonstration. Si $\alpha \in L$ est une racine d'ordre $n \geq 1$ de $f(X)$ alors il existe $g(X) \in L[X]$ tel que $f(X) = (X - \alpha)^n g(X)$ avec $g(\alpha) \neq 0$. La dérivée de $f(X)$ est alors donnée par $f'(X) = n(X - \alpha)^{n-1} g(X) + (X - \alpha)^n g'(X)$ et $f'(\alpha) = 0$ si $n \geq 2$ et $f'(\alpha) = g(\alpha) \neq 0$ si $n = 1$. Par conséquent, α est racine simple si et seulement si $f'(\alpha) \neq 0$. □

Théorème 3.56. *Soit $f(X) \in K[X]$ un polynôme irréductible.*

1. *Si K est de caractéristique 0 alors $f(X)$ est séparable.*
2. *Si K est de caractéristique $p > 0$ alors $f(X)$ séparable si et seulement si il n'existe pas $g(X) \in K[X]$ tel que $f(X) = g(X^p)$.*

Démonstration. 1) Supposons que $\mathrm{Car}(K) = 0$. Comme $f(X)$ est irréductible il est, à multiplication par une constante près (le polynôme minimal étant monique), le polynôme minimal de toutes ses racines. Il ne peut donc pas exister

4. Certains auteurs préfèrent dire qu'un polynôme est séparable s'il est irréductible et s'il ne possède que des racines simples. Dans tous les cas, les deux définitions coïncident pour les polynômes irréductibles.

de polynôme de degré inférieur à $f(X)$ avec une racine commune à $f(X)$. Soit $n = \deg(f(X))$ et soit $\alpha \in L$ une racine de $f(X)$ dans son corps de décomposition. Alors $\deg(f'(X)) < n$ avec $f'(X) \neq 0$, donc α ne peut être racine de $f'(X)$. Par la proposition précédente, α est racine simple de $f(X)$ et comme elle est arbitraire $f(X)$ est séparable.

2) Supposons que $\mathrm{Car}(K) = p > 0$. La grande différence avec le cas en caractéristique 0 est que $f'(X)$ peut être égal au polynôme nul. Dans ce cas $f'(X) = 0 = f'(\alpha)$ et α n'est pas racine simple de $f(X)$. Soit $f(X) = \sum_{i=0}^{n} a_i X^i$ son expression. Alors

$$f'(X) = \sum_{i=0}^{n} i a_i X^{i-1}$$

est le polynôme nul si et seulement si $ia_i = 0$ pour tout $0 < i < n$ (n'oublions pas qu'en caractéristique p les coefficients sont réduits modulo p). Ceci est possible si et seulement si $a_i = 0$ pour tout $i \not\equiv 0 \bmod p$. Ou encore, si et seulement si $f(X) = a_0 + a_p X^p + a_2 p X^{2p} + \cdots + a_{pm} X^{pm} = g(X^p)$ pour un certain $g(X) \in K[X]$. □

Définition 3.30. Un corps parfait est un corps dont toutes les extensions algébriques sont séparables.

Corollaire 3.57. *Si K est de caractéristique 0 alors il est parfait.*

Démonstration. Soit L/K une extension algébrique et soit $\alpha \in L$. Posons $m_\alpha(X)$ le polynôme minimal de α sur K. Par le théorème 3.56, $m_\alpha(X)$ est séparable. Comme α est arbitraire, cela montre que L/K est une extension séparable. □

Corollaire 3.58. *Si K est un corps fini alors il est parfait.*

Démonstration. Soit p la caractéristique de K. Soit L/K une extension algébrique et soit $\alpha \in L$. Vu le théorème 3.56, il s'agit de montrer que les polynômes de la forme $f(X) = g(X^p)$ ne sont pas irréductibles. Comme K est un corps fini de caractéristique p, $a = a^p$ pour tout $a \in K$. Par conséquent si $f(X) = \sum_{i=0}^{n} a_i X^{ip} = g(X^p)$ alors

$$f(X) = \sum_{i=0}^{n} a_i^p X^{ip} = \left(\sum_{i=0}^{n} a_i X^i \right)^p$$

et $f(X)$ n'est pas irréductible. Dès lors, le polynôme minimal de tout élément de L est séparable et K est parfait. □

Autrement dit, en pratique, les extensions sont toujours séparables et il faut aller chercher parmi les corps de caractéristique $p > 0$ de cardinal infini pour trouver des extensions non séparables (dans ce cas on parle d'extensions inséparables).

Example 3.59. Voici l'exemple le plus simple et le plus utilisé dans la littérature pour illustrer un exemple d'extension non séparable. Soit le corps $\mathbb{F}_p(t)$ des

fractions rationnels à coefficients dans $\mathbb{F}_p$ (i.e. ses éléments sont des quotients de polynômes à coefficients dans $\mathbb{F}_p$). Soit le polynôme $f(X) = X^p - t \in \mathbb{F}_p[t]$. L'idéal $\langle t \rangle \subset \mathbb{F}_p[t]$ est un idéal premier. Par conséquent, t joue le rôle d'un nombre premier p. Par le critère d'Eisenstein (généralisé), $f(X)$ est irréductible. Par le test de la dérivation $f'(X) = pX^{p-1} = 0$. Donc $f(X)$ est irréductible mais n'est pas séparable. Cela montre que $\mathbb{F}_p(t^{1/p})/\mathbb{F}_p(t)$ est une extension non séparable.

Proposition 3.60. *Soit L/K une extension finie. Alors les assertions suivantes sont équivalentes.*

1. $[L : K] = |Gal(L/K)|$
2. *L/K est une extension galoisienne.*
3. *L/K est une extension normale et séparable.*
4. *L est le corps de décomposition d'un ensemble de polynômes séparables de $K[X]$.*

Démonstration. On s'inspire de [22] (théorème 4.9) et [37] (théorème 2.7.14). Nous savons déjà que 1) $\iff$ 2). Pour le reste, on fait une preuve circulaire. 2) $\implies$ 3) Supposons que L/K est une extension galoisienne. Soit $\alpha \in L$ et considérons l'ensemble de ces conjugués $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$. Ceux-ci sont en nombre fini par le corollaire 3.50. Considérons le polynôme $f(X) = \prod_{i=1}^{n}(X - \alpha_i)$. Comme $\sigma(f(X)) = \prod_{i=1}^{n}(X - \sigma(\alpha_i)) = f(X)$ et que L/K est galoisienne on voit que $f(X) \in K[X]$. Par conséquent, le polynôme minimal de α divise $f(X)$ dans $K[X]$ et est séparable puisque $f(X)$ ne possède que des racines distinctes. En outre, toutes les racines de $f(X)$, et à fortiori de $m_\alpha(X)$, sont dans L. Par conséquent L/K est normale et séparable.

3) $\implies$ 4) Si L/K est normale et séparable alors le polynôme minimal de tout élément $\alpha \in L$ est séparable et scindé dans L. Donc L est le corps de décomposition de l'ensemble des polynômes minimaux de ses éléments.

4) $\implies$ 1) On fait une preuve par récurrence. Si $[L : K] = 1$ alors L/K est une extension galoisienne de K. Supposons maintenant que $[L : K] = n$. Par récurrence, on suppose que le résultat est vrai pour toute extension finie degré $< n$. Soit $S \subset K[X]$ l'ensemble des polynômes séparables dont L est le corps de décomposition et soit $f(X) \in S$ l'un d'eux. Comme $[L : K] > 1$, nous savons que $f(X)$ n'est pas un polynôme de degré 1 et donc qu'il possède au moins une racine $\alpha \notin K$. Soit l'extension $E = K(\alpha)$. Comme $K \subset E$ on a $[L : E] < n$. Mais l'extension L/E est encore le corps de décomposition de l'ensemble de polynômes séparables S où ces derniers sont vus comme des polynômes de $E[X]$. En utilisant la récurrence cela montre que L/E est une extension galoisienne. Soit $m_\alpha^K(X)$ le polynôme minimal de α sur K. Comme $m_\alpha^K(X)$ divise $f(X)$ nous savons que $m_\alpha^K(X)$ possède des racines distinctes. Soit m son degré et soient $\alpha_1, \ldots, \alpha_m$ ses racines. Nous savons donc que $[E : K] = m$. En outre, par le lemme 3.36, il existe m automorphismes $\sigma_i \in \mathrm{Gal}(L/K)$ tels que $\sigma_i(\alpha) = \alpha_i$. On montre que $|\mathrm{Gal}(L/K) : \mathrm{Gal}(L/E)| \geq m$ (l'indice du sous-groupe $\mathrm{Gal}(L/E)$ dans $\mathrm{Gal}(L/K)$ est supérieur ou égal à m). Pour voir cela il suffit de montrer que le groupe quotient $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/E) =$

$\{\sigma\mathrm{Gal}(L/E) \mid \sigma \in \mathrm{Gal}(L/K)\}$ possède au moins m classes distinctes. Supposons que $\sigma_i\mathrm{Gal}(L/E) \cap \sigma_j\mathrm{Gal}(L/E) \neq \emptyset$ pour un couple $i \neq j$. Soient $\theta, \gamma \in \mathrm{Gal}(L/E)$ tels que $(\sigma_1 \circ \theta)(\alpha) = (\sigma_2 \circ \gamma)(\alpha)$. Comme $\alpha \in E$ on sait que $\theta(\alpha) = \gamma(\alpha) = \alpha$. Dès lors $\alpha_i = \sigma_i(\alpha) = \sigma_i(\theta(\alpha)) = \sigma_j(\gamma(\alpha)) = \sigma_j(\alpha) = \alpha_j$ ce qui est une contradiction puisque $\alpha_i \neq \alpha_j$. Donc on a bien $|\mathrm{Gal}(L/K) : \mathrm{Gal}(L/E)| \geq m$. En outre [5]

$$\begin{aligned}
|\mathrm{Gal}(L/K)| &= |\mathrm{Gal}(L/E)||\mathrm{Gal}(L/K) : \mathrm{Gal}(L/E)| \text{ par Lagrange} \\
&\geq |\mathrm{Gal}(L/E)|.m, \text{ par ce précède} \\
&= [L : E][E : K], \text{ car L/E est galoisienne} \\
&= [L : K], \text{ par le théorème 3.23}
\end{aligned}$$

mais comme $|\mathrm{Gal}(L/K)| \leq [L : K]$ par le lemme 3.49, on a $|\mathrm{Gal}(L/K)| = [L : K]$, d'où la conclusion. □

Example 3.61. L'extension $\mathbb{F}_4/\mathbb{F}_2$ est une extension galoisienne. Pour voir cela, considérons le polynôme $f(X) = X^4 - X \in \mathbb{F}_2[X]$. Ce polynôme possède des racines distinctes par le test de la dérivation. En fait, l'ensemble des ses racines coïncide exactement avec l'ensemble des éléments de $\mathbb{F}_4$ car (voir exemple 3.25) $f(0) \bmod X^2 + X + 1$, $f(1) \bmod X^2 + X + 1$, $f(X) \bmod X^2 + X + 1$ et $f(X + 1) \bmod X^2 + X + 1$. Par conséquent, $\mathbb{F}_4$ est le corps de décomposition d'un polynôme séparable de $\mathbb{F}_2$, et par le résultat précédent, l'extension est galoisienne.

On peut vérifier les 3 autres caractérisations d'une extension galoisienne. Rappelons-nous que nous pouvions aussi définir l'ensemble des éléments de $\mathbb{F}_4$ comme $\{0, 1, \alpha, \alpha+1\}$ (voir l'exemple 3.25). Par ce qui précède $0, 1, \alpha, \alpha+1$ sont les racines de $f(X)$. Comme l'extension $\mathbb{F}_4/\mathbb{F}_2$ est de degré 2, le groupe de Galois $\mathrm{Gal}(\mathbb{F}_4/\mathbb{F}_2)$ a au plus 2 éléments. L'un deux est nécessairement l'identité. L'autre doit envoyer une racine de $f(X)$ sur une autre de ses racines. En particulier, si $\sigma \in \mathrm{Gal}(\mathbb{F}_4/\mathbb{F}_2)$ n'est pas l'identité, alors forcément $\sigma(\alpha) = \alpha + 1$. Clairement $\sigma^2 = \mathrm{id}$ et $\mathrm{Gal}(\mathbb{F}_4/\mathbb{F}_2) \cong \mathbb{Z}/2\mathbb{Z}$. Par conséquent, $|\mathrm{Gal}(\mathbb{F}_4/\mathbb{F}_2)| = [\mathbb{F}_4 : \mathbb{F}_2]$. Ensuite on a $\mathrm{Fix}(\mathrm{Gal}(\mathbb{F}_4/\mathbb{F}_2)) = \mathbb{F}_2$. Finalement, l'extension est normale et séparable. Pour la séparabilité, c'est automatique par le corollaire 3.58. Pour la normalité, tous les conjugués de tous les éléments de $\mathbb{F}_4$ sont dans $\mathbb{F}_4$. D'où la conclusion.

Remarque 3.62. La 4-ième caractérisation d'une extension galoisienne de la proposition précédente peut être lue de la façon suivante. Comme L/K est de degré fini, L est le corps de décomposition d'un nombre fini de polynômes séparables. En multipliant tous ces polynômes ensemble, on obtient un unique polynôme de sorte que cette caractérisation est équivalente à celle-ci : Une extension finie est galoisienne si et seulement si elle est le corps de décomposition d'un polynôme séparable. Lorsque le corps de base K est fini ou de caractéristique 0, nous avons vu que la séparabilité est automatique. Dans ce cas, cette

5. Le théorème de Lagrange de la théorie des groupes dit que si G est un groupe et H un sous-groupe de G alors $|G| = |G : H||H|$.

caractérisation se simplifie en : Une extension finie L/K est galoisienne si et seulement si L est le corps de décomposition d'un polynôme (non nul) de $K[X]$.

Corollaire 3.63. *Soit $K \subseteq E \subseteq L$ une tour d'extensions. Si L/K est une extension galoisienne alors L/E l'est aussi.*

Démonstration. Par la proposition précédente, L/K est une extension galoisienne si et seulement si L/K est une extension normale et séparable. Par les propositions 3.53 et 3.54 nous voyons que L/E est une extension normale et séparable. Par conséquent L/E est une extension galoisienne. □

Si ce corollaire paraît anodin, il est pourtant la clef pour montrer que la correspondance entre sous-groupes et corps intermédiaires d'une extension galoisienne est une bijection. C'est ce que nous allons voir dans le théorème fondamental suivant. Terminons avec un dernier lemme utilitaire.

Lemme 3.64. *Soit L/F une extension galoisienne. Soit $K \subseteq E \subseteq$ tel que $Fix(Gal(L/E)) = E$. Alors $\sigma(E) = Fix(\sigma Gal(L/E)\sigma^{-1})$ pour tout $\sigma \in Gal(L/K)$.*

Démonstration. On suit [37] (lemme 2.8.7). On montre d'abord que $\sigma(E) \subseteq \mathrm{Fix}(\sigma\mathrm{Gal}(L/E)\sigma^{-1})$. Soit $\alpha \in E$ et soit $\tau \in \mathrm{Gal}(L/E)$. Alors $\sigma\tau\sigma^{-1}\sigma(\alpha)$ et donc $\sigma(\tau(\alpha)) = \sigma(\alpha)$. Donc $\sigma(E) \subseteq \mathrm{Fix}(\sigma\mathrm{Gal}(L/E)\sigma^{-1})$. Inversement, si $\sigma\tau\sigma^{-1}(\beta) = \alpha$ pour un $\beta \in E$ et pour tout $\tau \in \mathrm{Gal}(L/E)$, alors $\tau\sigma^{-1}(\alpha) = \sigma^{-1}(\alpha)$. Dès lors, $\sigma^{-1}(\beta) = \alpha$ est fixé par $\mathrm{Gal}(L/E)$ et on voit que $\mathrm{Fix}(\sigma\mathrm{Gal}(L/E)\sigma^{-1}) \subseteq \sigma(E)$. □

3.7 Théorème fondamental de la théorie de Galois

Théorème 3.65. *(**Théorème fondamental de la théorie de Galois**) Soit L/K une extension galoisienne finie. Alors il existe une bijection entre l'ensemble des sous-groupes de $Gal(L/K)$ et l'ensemble des sous-corps intermédiaires de L/K de sorte que $F \leftrightarrow Gal(L/F)$ et $H \leftrightarrow F(H)$ avec $[L : F] = |H|$. Cette bijection vérifie $H_1 \subseteq H_2 \implies \Gamma(H_1) \supseteq \Gamma(H_2)$ pour tout sous-groupes H_1, H_2 de $Gal(L/K)$. De plus, si F est une extension intermédiaire entre L et K alors F/K est une extension galoisienne si et seulement si $Gal(K/F)$ est un sous-groupe normal de $Gal(L/K)$ et dans ce cas $Gal(F/K) \cong Gal(L/K)/Gal(L/F)$.*

Démonstration. Considérons la fonction

$$\Gamma : \mathcal{G} \to \mathcal{F} : H \mapsto \mathrm{Fix}(H)$$

qui associe à un sous-groupe de $\mathrm{Gal}(L/K)$ le corps fixé par celui-ci. Par la proposition 3.45, nous savons que cette fonction est injective. Montrons la surjectivité de Γ. Soit $K \subseteq E \subseteq L$ un corps intermédiaire de L/K. Par le corollaire 3.63 nous savons que L/E est aussi galoisienne. Par conséquent $E = \mathrm{Fix}(\mathrm{Gal}(L/E))$ et on a trouvé un sous-groupe de $\mathrm{Gal}(L/K)$ qui fixe E. Cela montre que Γ est une bijection entre l'ensemble des sous-groupes de $\mathrm{Gal}(L/K)$ et l'ensemble des corps intermédiaire de L/K.

Considérons le sous-groupe $\mathrm{Gal}(L/E)$ de $\mathrm{Gal}(L/K)$. Par le théorème de Lagrange $|H| = |\mathrm{Gal}(L/K)|/|\mathrm{Gal}(L/K) : H|$. De plus, $[L : K] = [L : E][E : K]$ par le théorème 3.23. Comme L/E et L/K sont galoisiennes, on sait par la proposition 3.60 que $[L : E] = |\mathrm{Gal}(L/E)|$ et $[L : E] = |\mathrm{Gal}(L/K)|$, dès lors

$$[E : K] = \frac{[L : K]}{[L : E]} = \frac{|\mathrm{Gal}(L/K)|}{\mathrm{Gal}(L/E)|} = |\mathrm{Gal}(L/K) : \mathrm{Gal}(L/E)|.$$

Reste à montrer le résultat sur les sous-groupes normaux. Supposons que $\mathrm{Gal}(L/E)$ est normal dans $\mathrm{Gal}(L/K)$. Par le lemme 3.64, nous savons que $\sigma(E) = \mathrm{Fix}(\sigma\mathrm{Gal}(L/E)\sigma^{-1})$ pour tout $\sigma \in \mathrm{Gal}(L/K)$ et comme $\mathrm{Gal}(L/E)$ est normal $\mathrm{Fix}(\sigma\mathrm{Gal}(L/E)\sigma^{-1}) = \mathrm{Fix}(\mathrm{Gal}(L/E)) = E$. Maintenant, l'homomorphisme $\theta : \mathrm{Gal}(L/K) \to \mathrm{Gal}(E/K)$ est surjectif par le théorème d'extension des isomorphismes. Son noyau est

$$\{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(x) = x \ , \forall x \in E\} = \mathrm{Gal}(L/E),$$

par conséquent $\mathrm{Gal}(E/K) \cong \mathrm{Gal}(L/K)/\mathrm{Gal}(L/E)$, ce qui achève la démonstration. □

Nous exposons, sans le démontrer, le théorème suivant.

Théorème 3.66. *(Théorème de l'élément primitif) Si L/K est une extension séparable finie, alors il existe un élément $\alpha \in L$ tel que $L = K(\alpha)$.*

On sait par les corollaires 3.57 et 3.58 que si K est de caractéristique 0, ou si K est un corps fini alors, en particulier, toutes ses extensions sont séparables et le théorème de l'élément primitif s'applique. Cela permet de se ramener dans les hypothèses du théorème 3.29, mais aussi de pouvoir déterminer tous les éléments de $\mathrm{Gal}(L/K)$ à partir de leur action sur un unique élément (α en l'occurrence).

Example 3.67. En reprenant l'exemple 3.47 on sait par le théorème de l'élément primitif que l'extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ peut en fait se réécrire comme $\mathbb{Q}(\alpha)/\mathbb{Q}$ pour un certain $\alpha \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$. On se convainc aisément que $\alpha = \sqrt{2} + \sqrt{3}$ convient.

3.8 Applications de la théorie de Galois classique

3.8.1 Extensions cyclotomiques

Dans cette section nous étudions les extensions cyclotomiques de $\mathbb{Q}$. Il est connu que l'ensemble des racines du polynôme $X^n - 1$ est

$$S_n = \left\{ e^{\frac{2i\pi j}{n}} \mid j = 0, 1, \ldots, n-1 \right\}.$$

Définition 3.31. Une racine primitive n-ième de l'unité sur $\mathbb{Q}$ est un élément $\zeta_n \in \overline{\mathbb{Q}}$ tel que $\zeta_n^n = 1$ mais $\zeta_n^m \neq 1$ pour tout $m < n$.

Les racines primitives n-ième de l'unité forment un sous-ensemble $P_n \subset S_n$. En fait, ce sont les racines $e^{\frac{2i\pi j}{n}}$ où j est premier à n car il est clair que si j/n se simplifie en a/b avec a et b premiers entre eux, alors $e^{\frac{2i\pi a}{b}}$ est une racine primitive b-ième avec $b < n$.

Définition 3.32. L'indicatrice d'Euler est la fonction

$$\phi : \mathbb{N}_0 \to \mathbb{N}_0 : n \mapsto \varphi(n) := \{m \in \mathbb{N}_0 \mid 0 < m < n \text{ et } m \nmid n\}$$

qui associe à tout entier non nul n le nombre d'éléments inférieurs à n et premiers à n.

Il faut compter 1 comme étant premier à tout élément (même à lui-même). Dès lors $\phi(1) = 1$ et on a par exemple $\phi(4) = 2$, $\phi(10) = 4$ et $\phi(p) = p - 1$ pour tout nombre premier p. Par définition, il y a $\phi(n)$ racines primitives n-ièmes de l'unité.

Définition 3.33. Le polynôme $\Phi_n(X) = \prod_{\zeta \in P_n}(X - \zeta) \in \mathbb{C}[X]$ est appelé le n-ième polynôme cyclotomique.

On voit directement que les polynômes cyclotomiques sont des polynômes moniques et que $\deg(\Phi_n(X)) = \phi(n)$ pour tout n.

Proposition 3.68. *Soit ζ_n une racine primitive n-ième de l'unité. Alors*
- *L'extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ est galoisienne.*
- $\Phi_n(X) \in \mathbb{Q}[X]$
- $X^n - 1 = \prod_{d|n} \Phi_d(X)$

Démonstration. Le polynôme $X^n - 1$ est séparable puisque ses racines sont distinctes. Comme $\zeta_n \in \mathbb{Q}(\zeta_n)$ on sait que $\zeta_n^m \in \mathbb{Q}(\zeta_n)$ pour tout $m \in \mathbb{Z}$. De plus, $\zeta_n = e^{\frac{2i\pi j}{n}}$ avec j premier à n, donc ζ_n^m parcourt toutes les racines de $X^n - 1$ lorsque m varie et clairement $\mathbb{Q}(\zeta_n)$ est le corps de décomposition de $X^n - 1$. Par conséquent $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ est le corps de décomposition d'un polynôme séparable et est donc une extension galoisienne. Si $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ alors $\sigma(\zeta_n) = \omega$ est une racine primitive n-ième de l'unité car $\sigma(\zeta_n^n) = \sigma(1) = 1 = \omega^n$ mais $\sigma(\zeta_n^m) = \omega^m \neq \sigma(1) = 1$ pour tout entier positif $m < n$. De ce fait

$$\sigma(\Phi_n(X)) = \prod_{\zeta \in P_n} (X - \sigma(\zeta)) = \Phi_n(X),$$

donc $\Phi_n(X) \in \mathbb{Q}[X]$. Finalement, si ζ est une racine de l'unité alors il existe un seul $d \in \mathbb{N}_0$ qui divise n tel que $\zeta = e^{\frac{2i\pi j}{d}}$ avec j premier à d, donc $X^n - 1 = \prod_{d|n} \Phi_d(X)$. □

Considérons quelques exemples.

Example 3.69. Les premiers polynômes cyclotomiques sont $\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$. Pour $n = 3$, on sait par la formule $X^n - 1 = \prod_{d|n} \Phi_d(X)$ que $X^3 - 1 = \Phi_1(X)\Phi_3(X)$ donc

$$\Phi_3(X) = \frac{X^3 - 1}{X - 1} = X^2 + X + 1.$$

Si $n = 4$, on peut déduire l'expression de $\Phi_4(X)$ à partir de la formule $X^4 - 1 = \Phi_1(X)\Phi_2(X)\Phi_4(X)$ mais on peut aussi le construire avec les racines primitives 4-ième de l'unité qui sont $e^{\frac{2i\pi}{4}}, e^{\frac{6i\pi}{4}}$ de sorte que

$$\begin{aligned}\Phi_4(X) &= \big(X - e^{\frac{2i\pi}{4}}\big)\big(X - e^{\frac{6i\pi}{4}}\big)\\ &= (X - i)(X + i)\\ &= X^2 + 1.\end{aligned}$$

Pour $n = 6$, on a

$$\begin{aligned}\Phi_6(X) &= \big(X - e^{\frac{2i\pi}{6}}\big)\big(X - e^{\frac{10i\pi}{6}}\big)\\ &= \left(X - \frac{1 + i\sqrt{3}}{2}\right)\left(X - \frac{1 - i\sqrt{3}}{2}\right)\\ &= X^2 - X + 1.\end{aligned}$$

On a vu par la proposition 3.68 que les polynômes cyclotomiques sont dans $\mathbb{Q}[X]$. On peut faire mieux : comme illustré dans l'exemple précédent, ceux-ci sont en fait dans $\mathbb{Z}[X]$.

Lemme 3.70 (Lemme de Gauss)**.** *Soient $f(X) = \sum_{i=0}^{n} a_i x^i$ et $g(X) = \sum_{i=0}^{m} b_i x^i$ des polynômes de $\mathbb{Z}[X]$ tel que $pgcd(a_0, \ldots, a_n) = 1$ et $pgcd(b_0, \ldots, b_m) = 1$. Alors $h(X) = \sum_{i=0}^{n+m} c_i x^i = f(X)g(X)$ est aussi tel que $pgcd(c_0, \ldots, c_{n+m}) = 1$.*

Démonstration. Supposons au contraire que $h(X)$ est tel que

$$\mathrm{pgcd}(c_0, \ldots, c_{n+m}) \neq 1.$$

Dans ce cas, il existe un nombre premier p qui divise chacun des $c_0, \ldots, c_{n+m}$. Par les hypothèses sur $f(X)$, il existe un plus petit indice $1 \leq i \leq n$ tel que a_i n'est pas divisible par p mais tel que p divise $a_{i-1}, a_{i-2}, \ldots, a_0$. De même, pour $g(X)$ il existe un plus petit indice $1 \leq j \leq m$ tel que p ne divise pas b_j mais tel que p divise $b_{j-1}, b_{j-2}, \ldots, b_0$. En développant le produit $f(X)g(X)$ on a que le coefficient de X^{i+j} est

$$c_{i+j} = a_i b_j + a_{i+1} b_{j-1} + a_{i+2} b_{j-2} + \cdots + a_{i-1} b_{j+1} + a_{i-2} b_{j+2} + \ldots$$

de sorte que $p | c_{i+j}$ mais aussi $p | a_k$ et $p | b_l$ pour tout $k < i$ et pour tout $l < j$. Par conséquent, le terme restant $a_i b_j$ est aussi divisible par p. Comme p est premier, on en conclut que $p | a_i$ ou $p | b_j$ ce qui est en contradiction avec l'hypothèse. □

Lemme 3.71. *Soit $h(X) \in \mathbb{Z}[X]$ un polynôme monique et soient deux polynômes moniques $f(X), g(X) \in \mathbb{Q}[X]$ tel que $h(X) = f(X)g(X)$. Alors $f(X), g(X) \in \mathbb{Z}[X]$.*

Démonstration. Posons $f(X) = \sum_{i=0}^{n} a_i x^i$ et $g(X) = \sum_{i=0}^{m} b_i x^i$. Soit p_1 le plus petit commun multiple des dénominateurs des coefficients a_i. De même, soit p_2 le plus petit commun multiple des dénominateurs des coefficients b_j. Comme $f(X)$

et $g(X)$ sont moniques, on a $\text{pgcd}(p_1a_0, \ldots, p_1a_n) = 1$ et $\text{pgcd}(p_2b_0, \ldots, p_2b_m) = 1$. Par conséquent

$$p_1p_2h(X) = (p_1f(X))(p_2g(X)) \in \mathbb{Z}[X]$$

et par le lemme de Gauss les coefficients du polynôme $(k_1f(X))(k_2g(X))$ sont premiers entre eux. Donc la seule possibilité est que $p_1p_2 = 1$, c'est-à-dire $p_1 = 1$ et $p_2 = 1$. □

En prenant la contraposée, ce lemme signifie aussi que si $h(X) \in \mathbb{Z}[X]$ est un polynôme monique irréductible sur $\mathbb{Z}[X]$ alors il est irréductible sur $\mathbb{Q}[X]$.

Proposition 3.72. *Pour tout $n \geq 1$ $\Phi_n(X) \in \mathbb{Z}[X]$.*

Démonstration. La démonstration se fait par récurrence. On a vu que $\Phi_1(X) = X - 1 \in \mathbb{Z}[X]$. Supposons que $\Phi_m(X) \in \mathbb{Z}[X]$ pour tout $m < n$. Par la formule de la proposition 3.68 on a

$$X^n - 1 = \Phi_n(X) \prod_{d|n, d<n} \Phi_d(X)$$

et comme $X^n - 1 \in \mathbb{Z}[X]$, $\prod_{d|n,d<n} \Phi_d(X) \in \mathbb{Z}[X]$ et $\Phi_n(X) \in \mathbb{Q}[X]$ sont moniques on en déduit que $\Phi_n(X) \in \mathbb{Z}[X]$ par le lemme précédent. □

Proposition 3.73. *Les polynômes cyclotomiques sont irréductibles sur $\mathbb{Q}[X]$.*

Cette preuve est celle que l'on trouve quasiment dans tous les ouvrages sur la théorie de Galois.

Démonstration. Supposons que $\Phi_n(X)$ n'est pas irréductible sur $\mathbb{Q}$. Alors par le lemme 3.71 $\Phi_n(X)$ n'est pas irréductible sur $\mathbb{Z}[X]$ et il existe des polynômes moniques $f(X), g(X) \in \mathbb{Z}[X]$ tel que $\Phi_n(X) = f(X)g(X)$ avec $f(X)$ irréductible sur $\mathbb{Z}[X]$. Les polynômes $f(X)$ et $\Phi_n(X)$ possèdent un certain nombre de racines communes. On va montrer que $f(X)$ possède en fait toutes les racines de $\Phi_n(X)$ ce qui montrera l'irréductibilité de $\Phi_n(X)$ sur $\mathbb{Z}[X]$ et donc, par la contraposée du lemme 3.71, sur $\mathbb{Q}[X]$.

La première étape consiste à montrer que si ζ est une racine de $f(X)$ alors ζ^p est aussi une racine de $f(X)$ pour tout p premier à n. Supposons qu'il existe p premier à n tel que ζ^p n'est pas racine de $f(X)$. Alors ζ^p est racine de $g(X)$ (car ζ^p est racine de $\Phi_n(X)$) et ζ est racine de $g(X^p)$. Comme $f(X)$ est un polynôme monique irréductible, c'est le polynôme minimal de ζ et $f(X)$ divise $g(X^p)$ dans $\mathbb{Z}[X]$. Considérons l'homomorphisme

$$\phi : \mathbb{Z}[X] \to \mathbb{F}_p[X] : f(X) = \sum_{i=0}^{n} a_i x^i \mapsto \phi(f(X)) := \overline{f}(X) = \sum_{i=0}^{n} \overline{a}_i x^i$$

qui réduit les coefficients d'un polynôme modulo p. Alors

$$\begin{aligned}\overline{g}(X^p) &= \sum_{i=0}^{m} \overline{b}_i x^{ip} \\ &= \sum_{i=0}^{m} \overline{b}_i^p x^{ip} \text{ car } \overline{b}^p \equiv \overline{b} \bmod p \quad \forall \overline{b} \in \mathbb{F}_p \\ &= \left(\sum_{i=0}^{m} \overline{b}_i x^i \right)^p \text{ car } (x+y)^p = x^p + y^p \text{ dans } \mathbb{F}_p \\ &= (\overline{g}(X))^p\end{aligned}$$

et $\overline{f}(X)$ divise $(\overline{g}(X))^p$ dans $\mathbb{F}_p[X]$. Soit $\overline{l}(X) \in \mathbb{F}_p[X]$ un facteur irréductible de $\overline{f}(X)$. Alors $\overline{l}(X)|\overline{f}(X)$ et $\overline{l}(X)|(\overline{g}(X))^p$ donc $\overline{l}(X)|\overline{g}(X)$. Par conséquent, l'égalité $\overline{\Phi}_n(X) = \overline{f}(X)\overline{g}(X)$ montre que $\overline{l}^2(X)$ divise $\overline{\Phi}_n(X)$. Or $\overline{\Phi}_n(X)$ est un facteur de $X^n - \overline{1}$ qui ne possède pas de racines multiples. En effet, $nX^{n-1} \not\equiv 0 \bmod p$ (car $p \nmid n$ par hypothèse) et $X^n - \overline{1}$ est premier avec nX^{n-1}. Cela montre que $\overline{\Phi}_n(X)$ ne possède pas de racines multiples et que l'hypothèse qu'il existe un p tel que ζ^p n'est pas une racine de $f(X)$ est fausse. Maintenant, toutes les racines de $\Phi_n(X)$ s'écrivent comme ζ^m pour m premier à p. Si on décompose $m = p_1 p_2 \dots p_m$ en un produit de nombres premiers, on sait que $p_1, p_2, \dots, p_m$ sont tous premiers à n de sorte que $\zeta^m = \zeta^{p_1,\dots,p_n} = \zeta^{p_1(p_2 \cdots p_m)}$ est encore une racine de $f(X)$ car ζ^{p_1} est une racine de $f(X)$, $(\zeta^{p_1})^{p_2}$ est aussi une racine de $f(X)$ etc... On en conclut que $f(X) = \Phi_n(X)$ est irréductible. □

Rappelons que le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ désigne l'ensemble des entiers modulo n, premiers à n et munis de la multiplication modulo n. Par exemple $(\mathbb{Z}/6\mathbb{Z})^\times = \{1, 5\}$ et notons que $5^2 \bmod 6 = 1$, donc cela forme bien un groupe. On voit directement que l'ordre de ce groupe est $\phi(n)$.

Théorème 3.74. *Soit ζ_n une racine primitive n-ième de l'unité. L'extension galoisienne $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ est de degré $\phi(n)$, son groupe de galois est Gal$(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.*

Démonstration. Le polynôme minimal de ζ_n est $\Phi_n(X)$ qui est de degré $\phi(n)$ donc $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$. Maintenant si $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ alors $\sigma(\zeta_n) = \zeta_n^m$ où m est déterminé par le choix de σ. La fonction

$$\omega : \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times : \sigma \mapsto m_\sigma + n\mathbb{Z}$$

est un homomorphisme de groupes car si $\sigma, \tau \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ alors $\sigma(\tau(\zeta_n)) = \sigma(\zeta_n^{m_\tau}) = \zeta_n^{m_\sigma m_\tau}$ c'est-à-dire $\omega(\sigma\tau) = m_\sigma m_\tau = \omega(\sigma)\omega(\tau)$. Si $\omega(\sigma) = 1$ alors $\sigma(\zeta_n) = \zeta_n$ donc $\sigma = id$ et ω est un homomorphisme injectif. Finalement, $\text{Card}(\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n) = \text{Card}((\mathbb{Z}/n\mathbb{Z})^\times) < +\infty$ donc l'homomorphisme est aussi surjectif (principe du tiroir). On a donc $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. □

Example 3.75. Prenons $n = 5$ et posons $\zeta_5 = e^{\frac{2i\pi}{5}}$. L'extension $\mathbb{Q}(\zeta_5)/\mathbb{Q}$ est de degré $\phi(5) = 4$. Le polynôme minimal de ζ_5 est

$$\Phi_5(X) = \frac{X^5 - 1}{X - 1} = X^4 + X^3 + X^2 + X + 1.$$

Par le théorème fondamental de la théorie de Galois, les sous-extensions de $\mathbb{Q}(\zeta_5)/\mathbb{Q}$ sont en bijection avec les sous-groupes de $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \cong (\mathbb{Z}/5\mathbb{Z})^\times$. Ce groupe est cyclique. En effet $(\mathbb{Z}/5\mathbb{Z})^\times = \{1, 2, 3, 4\}$ et on voit que 2 génère ce groupe car 2 mod 5, $2^2 \equiv 4 \bmod 5$, $2^3 \equiv 3 \bmod 5$ et $2^4 \equiv 1 \bmod 5$. Dès lors $(\mathbb{Z}/5\mathbb{Z})^\times = \langle 2 \rangle$ et les sous-groupes de $(\mathbb{Z}/5\mathbb{Z})^\times$ sont donc aussi cycliques. En fait il n'y en a qu'un seul non trivial et il est donné par $\langle 4 \rangle$. Par la bijection donnée par ω dans la preuve du théorème 3.74, 2 correspond à l'élément du groupe de Galois σ tel que $\sigma(\zeta_5) = \zeta_5^2$ donc $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) = \langle \sigma \rangle$ et son unique sous-groupe est $\langle \sigma^2 \rangle$. Le polynôme minimal sur le corps fixé par $\langle \sigma^2 \rangle$ est

$$\begin{aligned}(X - \zeta_5)(X - \sigma^2(\zeta_5)) &= (X - \zeta_5)(X - \zeta_5^4) \\ &= X^2 + \frac{1 - \sqrt{5}}{2} X + 1.\end{aligned}$$

Or, ce polynôme est dans $\mathbb{Q}(\frac{1-\sqrt{5}}{2})[X] = \mathbb{Q}(\frac{1-\sqrt{5}}{2})[X]$ et le polynôme minimal de $\frac{1-\sqrt{5}}{2}$ est de degré 2 sur $\mathbb{Q}$ donc la correspondance galoisienne est donnée par le diagramme suivant.

$$\begin{array}{ccc} \mathbb{Q}(\zeta_5) & & 1 \\ \Big| 2 & & \Big| 2 \\ \mathbb{Q}\big(\frac{1-\sqrt{5}}{2}\big) = \mathbb{Q}(\sqrt{5}) & & \langle \sigma^2 \rangle \\ \Big| 2 & & \Big| 2 \\ \mathbb{Q} & & \langle \sigma \rangle \end{array}$$

3.8.2 Résolubilité par radicaux

Dans cette section, tous les corps sont supposés de caractéristique 0.

Le sujet de cette section est le théorème dû à Galois qui donne une condition nécessaire et suffisante pour qu'un polynôme soit résoluble par radicaux. Les anciens étaient soucieux de l'exactitude de leurs calculs et souhaitaient déterminer les racines d'un polynôme de manière exacte (c'est-à-dire sans approximations numériques). L'avantage des expressions algébriques par radicaux est que l'on ne perd pas de précision en effectuant des opérations classiques (Par exemple $(\sqrt{2})^2 = 2$ alors que $(\sqrt{2})^2 \approx (1.4142)^2 = 1.99996164 \approx 2$). Après avoir résolu de manière exacte les polynômes de degré deux, trois et quatre, les mathématiciens pensaient pouvoir donner une expression exacte pour le polynôme générique de

degré cinq. Galois lui-même cru résoudre ce dernier, mais se rétracta pour finalement démontrer qu'il existe en fait certains polynômes de degré cinq avec des racines qui ne s'expriment pas "gentillement" en fonction des coefficients de ce polynôme. Aujourd'hui, peu de gens utilisent les formules de Ferrari pour exprimer les racines d'un polynôme de degré quatre de manière exacte, et de fait, l'ordinateur permet d'obtenir des précisions de l'ordre de 10^{-16} aisément. D'autres expressions moins restrictives que d'exprimer des racines de polynômes par radicaux ont été envisagées. Il se trouve que pour tout polynôme de degré quelconque à coefficient dans un corps $K \subseteq \mathbb{C}$, on peut exprimer les racines à l'aide de fonctions elliptiques.

La première étape est de formaliser la notion de résolubilité par radicaux. Soit $f(X) \in K[X]$ un polynôme non constant. Initialement, la question est de savoir si les racines de $f(X)$ peuvent s'écrire en terme de combinaisons de sommes, de produits, de soustractions, de quotients et de racines n-ièmes des coefficients de $f(X)$. Les quatre première opérations sont celles qui apparaissent naturellement dans un corps. La dernière apparaît lorsque l'on adjoint des racines n-ième des éléments de ce corps (ici K) pour obtenir une extension de K. Prenons $K = \mathbb{Q}$ et considérons le nombre

$$\frac{1}{5}\left(\sqrt[3]{1+\sqrt{2}+\sqrt{3}}-4\right).$$

Cet élément appartient à une extension de $\mathbb{Q}$ qui peut être obtenue à partir de $\mathbb{Q}$ en adjoignant $\sqrt{2}$ puis $\sqrt{3}$ puis $\sqrt[3]{1+\sqrt{2}+\sqrt{3}}$ successivement. On obtient ainsi une tour d'extensions

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2},\sqrt{3}) \subset \mathbb{Q}\left(\sqrt[3]{1+\sqrt{2}+\sqrt{3}}\right),$$

et à chaque étape, on ne fait que rajouter une racine k-ième d'un élément du corps précédent. Ce constat éclaire les deux définitions suivantes.

Définition 3.34. Une extension L/K est dite radicale s'il existe une tour d'extensions

$$K = E_1 \subset E_2 \subset \cdots \subset E_n = L$$

telle que $E_{i+1} = E_i(\alpha_i)$ où $\alpha_i = a_i^{n_i}$ avec $a \in E_i$ et $n_i \in \mathbb{N}$ pour tout $1 \leq i \leq n-1$.

Définition 3.35. Un polynôme non constant $f(X) \in K[X]$ est résoluble par radicaux si son corps de décomposition est une sous-extension d'une extension radicale de K.

Pour une première lecture, la définition suivante semble sortir de nul part. Le lecteur verra que cette définition apparaît naturellement dans le théorème de Galois sur la résolubilité par radicaux.

Définition 3.36. Un groupe G est résoluble s'il existe une suite de sous-groupes

$$G = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_{n-1} \supseteq H_n = \langle 1 \rangle,$$

avec H_i normal dans H_{i+1} et H_{i+1}/H_i abélien pour tout $i = 0, \ldots, n-1$. De manière équivalente on peut demander que chaque H_{i+1}/H_i soit cyclique.

Démonstration. Voir [16]. □

On peut cependant se raccrocher aux définitions précédentes en voyant qu'il est question de tour d'extensions, d'extensions galoisiennes et donc, par le théorème fondamental de la théorie, d'une suite de sous-groupes vérifiants certaines propriétés.

Example 3.76. Tout groupe abélien fini est résoluble.

Proposition 3.77. *Soit G un groupe et soit $H \subseteq G$ un sous-groupe normal. Alors G est résoluble si et seulement si H et G/H sont résolubles.*

Démonstration. C'est à nouveau un résultat de la théorie des groupes. (Voir [16].) □

Proposition 3.78. *Soit K un corps contenant une racine primitive n-ième de l'unité. Soit $f(X) = X^n - a \in K[X]$ et soit L le corps de décomposition de $f(X)$. Alors L/K est une extension galoisienne et $Gal(L/K)$ est cyclique. En particulier $Gal(L/K)$ est résoluble.*

Démonstration. Si $a = 0$ le cas est trivial. Supposons que $a \neq 0$. Le polynôme $X^n - a$ est séparable. En effet, par le test de la dérivée, nX^{n-1} ne possède pas de racines communes à $X^n - a$. Or le corps de décomposition d'un polynôme séparable est une extension galoisienne, donc L/K est galoisienne.

Soit $\zeta_n \in K$ une racine primitive n-ième de l'unité. Les racines de $X^n - a$ sont $\sqrt[n]{a}, \zeta_n \sqrt[n]{a}, \ldots, \zeta_n^{n-1} \sqrt[n]{a}$. Par conséquent, le seul élément à adjoindre à K pour obtenir le corps de décomposition est $\sqrt[n]{a}$. On a donc $L = K(\sqrt[n]{a})$. Soit $\sigma \in \mathrm{Gal}(L/K)$. Son action sur L ne va dépendre que de la valeur de $\sigma(\sqrt[n]{a})$, qui est une racine de $X^n - a$. Il existe donc un $0 \leq i \leq n-1$ tel que $\sigma(\sqrt[n]{a}) = \zeta_n^i \sqrt[n]{a}$. Soit $\tau \in \mathrm{Gal}(L/K)$ avec $\sigma \neq \tau$. Alors, il existe encore un $0 \leq j \leq n-1$ tel que $\sigma(\sqrt[n]{a}) = \zeta_n^j \sqrt[n]{a}$. Dès lors la composition $(\sigma \circ \tau)(\sqrt[n]{a}) = \zeta_n^{i+j} \sqrt[n]{a} = \zeta_n^{i+j \bmod n} \sqrt[n]{a}$ montre que l'application

$$\theta : \mathrm{Gal}(L/K) \to \mathbb{Z}/n\mathbb{Z}$$

qui associe à σ la puissance i de $\sigma(\sqrt[n]{a})/\sqrt[n]{a} = \zeta^i$ est un homomorphisme de groupe. Supposons que $\theta(\sigma) = 0$, alors $\sigma(\sqrt[n]{a}) = \sqrt[n]{a}$ et $\sigma = \mathrm{id}$ par conséquent θ est injectif et $\mathrm{Gal}(L/K)$ est isomorphe à un sous-groupe du groupe cyclique $\mathbb{Z}/n\mathbb{Z}$. Cela montre que $\mathrm{Gal}(L/K)$ est lui aussi cyclique. Comme tout groupe cyclique est abélien et que tout groupe abélien est résoluble, on a la conclusion. □

Une extension galoisienne dont le groupe de Galois est cyclique est appelée une extension cyclique.

Théorème 3.79. *(Théorème de Hilbert 90) Soit L/K une extension cyclique de degré n. Soit $\sigma \in Gal(L/K)$ un générateur du groupe. Alors $\prod_{i=1}^{n} \sigma^i(\alpha) = 1$ si et seulement si $\alpha\sigma(\beta) = \beta$ pour un $\beta \in L$.*

Nous ne démontrons pas ce théorème mais la preuve peut être trouvée dans [22].

Proposition 3.80. *Soit K un corps contenant une racine primitive n-ième de l'unité. Si L/K est une extension cyclique de degré n alors il existe $a \in K$ tel que $L = K(\sqrt[n]{a})$.*

Démonstration. Soit σ un générateur de $\mathrm{Gal}(L/K)$. Alors $\prod_{i=1}^{n} \sigma^i(\zeta_n) = 1$ car c'est égal au terme indépendant du polynôme minimal de ζ_n. Par le théorème de Hilbert 90 il existe donc $\alpha \in L$ tel que $\sigma(\alpha) = \zeta_n \alpha$. Comme $\zeta_n \in K$ on sait que $\sigma^i(\alpha) = \zeta^i \alpha$ pour tout $1 \leq i \leq n$. En outre $\sigma(\alpha^n) = \sigma(\alpha)^n = (\zeta\alpha)^n = \alpha^n$ donc $\alpha^n \in K$. Par conséquent $L = K(\alpha)$. □

Proposition 3.81. *Soient K un corps et $f(X) = X^n - a \in K[X]$. Si L est le corps de décomposition de $f(X)$ alors L/K est une extension galoisienne et $Gal(L/K)$ est résoluble.*

Démonstration. Soit ζ_n une racine primitive n-ième de l'unité. Notons la différence avec la propriété précédente. Ici K ne contient pas forcément ζ_n. On va donc supposer que K ne contient pas ζ_n (sinon on se ramène à la propriété précédente). Par le même raisonnement que précédemment, $X^n - a$ est séparable, mais son corps de décomposition est $L = K(\sqrt[n]{a}, \zeta_n)$. À nouveau L/K est une extension galoisienne. Considérons la tour d'extension $K \subset K(\zeta_n) \subset L$. L'extension $L/K(\zeta_n)$ est cyclique par la propriété précédente. En particulier $\mathrm{Gal}(L/K(\zeta_n))$ est abélien. On montre que $\mathrm{Gal}(K(\zeta_n)/K)$ est aussi abélien. Soit $\sigma \in \mathrm{Gal}(K(\zeta_n)/K)$. Alors σ est entièrement déterminé par la valeur $\sigma(\zeta_n)$ et il existe $0 \leq i \leq n-1$ tel que $\sigma(\zeta_n) = \zeta_n^i$. Soit $\tau \in \mathrm{Gal}(K(\zeta_n)/K)$. Alors il existe encore un $0 \leq j \leq 1$ tel que $\tau(\zeta_n) = \zeta_n^j$. Cela montre que $(\sigma \circ \tau)(\zeta_n) = \zeta_n^{i+j} = (\tau \circ \sigma)(\zeta_n)$ et on peut étendre ce résultat pour tout $\alpha \in K(\zeta_n)$ de sorte que $\mathrm{Gal}(K(\zeta_n)/K)$ est abélien. Maintenant, par le théorème fondamental de la théorie de Galois, $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/K(\zeta_n)) \cong \mathrm{Gal}(K(\zeta_n)/K)$ est abélien. Par conséquent $\mathrm{Gal}(L/K) \supseteq \mathrm{Gal}(L/K(\zeta_n)) \supseteq \langle 1 \rangle$ est une suite de sous-groupes comme dans la définition de groupe résoluble et $\mathrm{Gal}(L/K)$ est résoluble. □

Dans la preuve précédente, on aurait pu aussi se convaincre que $\mathrm{Gal}(K(\zeta_n)/K)$ est abélien par le fait que le quotient d'un groupe abélien par un de ses sous-groupe est toujours abélien.

Lemme 3.82. *Si L/K est une extension radicale et si on note E la clôture normale de L alors E est une extension radicale de K.*

Démonstration. On montre d'abord que si E_1/K et E_2/K sont deux extensions radicales de K alors E_1E_2 aussi. Par hypothèse il existe une tour d'extension

$$K = F_1 \subseteq F_2 \subseteq \cdots \subseteq F_n = E_1$$

et de même

$$K = F_1' \subseteq F_2' \subseteq \cdots \subseteq F_n' = E_1$$

avec $F_{i+1} = F_i(\sqrt[n_i]{a_i})$ pour $a_i \in F_i$ et $F'_{i+1} = F'_i(\sqrt[m_i]{b_i})$ pour $b_i \in F'_i$ pour chaque i. Dès lors

$$K \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq E_1 \subseteq E_1F'_1 \subseteq E_1F'_2 \subseteq \cdots \subseteq E_2.$$

Maintenant $E_1F'_1 = E_1(\sqrt[m_1]{b_1})$ et $b_1 \in K$ par hypothèse, donc $b_1 \in E_1$ et cette extension est bien une extension radicale. Cela montre que la tour d'extensions est encore une extension radicale. Pour montrer que la clôture normale de L est une extension radicale de K, il suffit de savoir que la clôture normale est la composition de l'ensemble des $\sigma(L)$ pour $\sigma \in \mathrm{Gal}(E/K)$. Par ce qui précède, $E = \sigma_1(L)\ldots\sigma_k(L)$ où σ_k parcourt l'ensemble de $\mathrm{Gal}(E/K)$ est à nouveau une extension radicale de K. □

Théorème 3.83. *(Condition nécessaire et suffisante de résolubilité par radicaux) Soit $f(X) \in K[X]$ et soit L son corps de décomposition. Alors $f(X)$ est résoluble par radicaux si et seulement si $Gal(L/K)$ est résoluble.*

Démonstration. Sans perte de généralité, on peut supposer que $f(X)$ est séparable.

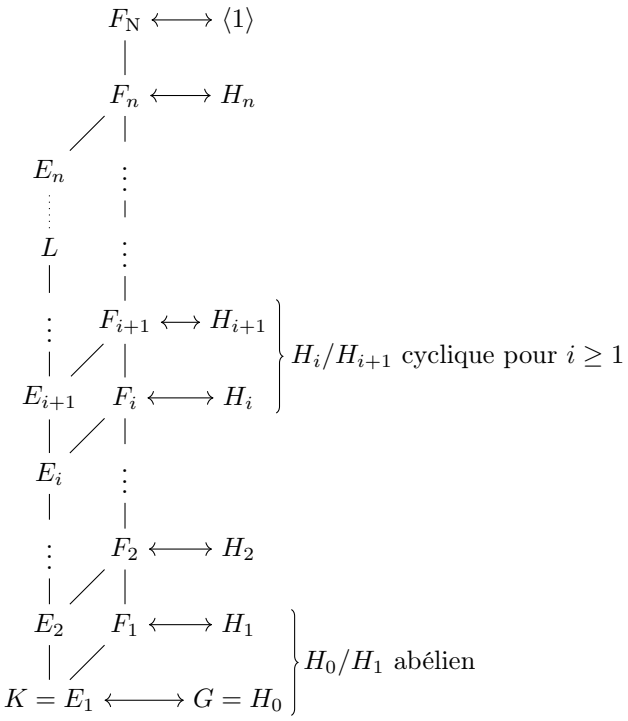
1) Supposons dans un premier temps que $f(X)$ est résoluble. Par définition, il existe une tour d'extensions

$$K = E_1 \subset E_2 \subset \cdots \subset E_n,$$

où $E_{i+1} = E_i(\sqrt[n_i]{a_i})$ avec $a_i \in E_i$ et $n_i \in \mathbb{N}$ pour tout $1 \leq i \leq n-1$ tel que $L \subset E_n$. Soit m le plus petit commun multiple de tous les n_i. Soit ζ une racine primitive m-ième de l'unité et considérons les extensions $F_i = E_i(\zeta)$ pour tout $1 \leq i \leq n$. Maintenant F_n n'est pas nécessairement une extension galoisienne de K. Par lemme précédent la clôture normale F_N de F_n est à la fois une extension radicale et une extension galoisienne de K. En outre l'extension F_N/K contient toujours le corps de décomposition de $f(X)$. Posons $G = H_0 = \mathrm{Gal}(F_N/K)$ et plus généralement $H_i = \mathrm{Gal}(F_N/F_i)$ pour tout $1 \leq i \leq n$. On a la suite de sous-groupes suivante

$$G = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_n \supseteq \langle 1 \rangle.$$

Par la proposition 3.78 les extensions $F_{i+1} = F_i(\sqrt[n_i]{a_i})$ sont cycliques pour tout $1 \leq i \leq n-1$ (chacun des F_i contenant ζ, il contient en particulier une racine primitive n_i-ième de l'unité). Par conséquent chaque H_{i+1} est un sous-groupe abélien de H_i. De plus, la preuve de la proposition 3.81 montre que l'extension F_1/K est galoisienne et $\mathrm{Gal}(F_1/K) \cong H_0/H_1$ est abélien. De plus, les quotients H_i/H_{i+1} étant cycliques pour $1 \leq i \leq n-1$ (et donc abéliens), on en conclut que $\mathrm{Gal}(F_N/K)$ est résoluble. Comme $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(F_N/K)/\mathrm{Gal}(F_N/L)$ la proposition 3.77 montre que $\mathrm{Gal}(L/K)$ est résoluble. Le diagramme suivant illustre la situation.



2) Supposons que $G = \mathrm{Gal}(L/K)$ est résoluble. Posons $[L : K] = n$ et soit ζ une racine primitive n-ième de l'unité. Considérons les extensions $F = K(\zeta)$ et $L' = L(\zeta)$. Dès lors $H = \mathrm{Gal}(L'/F)$ est un sous-groupe du groupe résoluble G et est donc lui-même résoluble. Par la (deuxième) définition de groupe résoluble, il existe une suite de sous-groupes

$$H = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_m = \langle 1\rangle,$$

tel que H_{i+1} est un sous-groupe abélien de H_i et H_i/H_{i+1} est cyclique pour tout $1 \leq i \leq m-1$. Par le théorème fondamental de la théorie de Galois il existe une tour d'extension

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_m = L'$$

tel que $F_i = \mathrm{Fix}(H_i)$ pour tout $1 \leq i \leq m$. De plus chaque $\mathrm{Gal}(F_{i+1}/F_i) = H_i/H_{i+1}$ est cyclique et (comme chaque F_i contient ζ) par la proposition 3.80, $F_{i+1} = F_i(\sqrt[n_i]{a_i})$ pour tout i de sorte que la tour d'extension est une extension radicale L'/F contenant le corps de décomposition de $f(X)$. Par conséquent $f(X)$ est résoluble. □

L'application classique de ce résultat se base sur les propositions suivantes. Rappelons qu'un groupe G est simple s'il ne possède aucun sous-groupe normal autre que $\langle 1\rangle$ ou éventuellement lui-même.

Proposition 3.84. *Si G est un groupe simple non abélien, alors il n'est pas résoluble.*

Démonstration. Comme G est simple, il ne possède pas de sous-groupe normal autre que lui-même et $\langle 1 \rangle$. On a donc l'unique suite $G \supseteq \langle 1 \rangle$. Mais G n'est pas abélien, donc $G/\langle 1 \rangle$ n'est pas abélien et G n'est pas résoluble. □

Proposition 3.85. *Le groupe alterné A_n est simple et non abélien.*

Démonstration. Voir par exemple [37] corollaire $A.3.6$ ou encore [31] théorème 14.7. □

Proposition 3.86. *Le groupe S_n n'est pas résoluble pour $n \geq 5$.*

Démonstration. Le groupe S_n contient A_n comme sous-groupe, or tout sous-groupe d'un groupe résoluble est résoluble. Donc S_n n'est pas résoluble. □

Cela implique que le polynôme général de degré 5 n'est pas résoluble par radicaux car il existe des polynômes de degré 5 dont le groupe de Galois est S_5.

Proposition 3.87. *Le groupe S_5 est généré par un élément d'ordre 2 et un élément d'ordre 5.*

Corollaire 3.88. *Soit $f(X) \in \mathbb{Q}[X]$ un polynôme irréductible de degré 5. Si $f(X)$ possède 3 racines réelles et 2 racines complexes (donc conjugées) alors $f(X)$ n'est pas résoluble par radicaux.*

Démonstration. Soit L le corps de décomposition de $f(X)$. Le résultat découle de ce que $\mathrm{Gal}(L/K)$ contient la conjugaison $\sigma = a + ib \mapsto a - ib$ et de ce que le degré $[L : K]$ est un multiple de 5. Comme la conjugaison est d'ordre 2 et que le théorème de Cauchy [6] nous dit qu'il existe un élément de $\mathrm{Gal}(L/K)$ d'ordre 5, on sait que $\mathrm{Gal}(L/K) \cong S_5$. □

Example 3.89. Par le critère d'Eisenstein le polynôme $x^5 - 4x + 2$ est irréductible. Ses racines sont $\approx 0.5\ldots, -1.5\ldots, 1.2\ldots$ et $-0.1 + 1.4i$, $-0.1 - 1.4i$. Par conséquent, ce polynôme n'est pas résoluble par radicaux.

3.8.3 Construction à la règle et au compas

On se donne un feuille blanche, et sur celle-ci sont fixés deux points définis comme constructibles, distants d'une unité. À cela, on ajoute un compas qui ne peut être centré qu'en un point déjà construit et qui ne peut tracer que des cercles passant par des points déjà construits. Finalement, nous avons aussi accès à une règle ne pouvant relier que des points déjà construits. Les intersections entre les droites et les cercles tracés sont des nombres dits constructibles. Avec ces outils, les mathématiciens de la Grèce antique pensaient pouvoir tracer toutes les constructions géométriques possibles. Cependant, trois d'entre elles se révèlent plus difficiles que les autres et il faudra attendre le 19-ième siècle pour que les mathématiciens démontrent leur impossibilité. Les questions sont : Avec une règle et un compas, est-il possible de

6. Soit G un groupe fini d'ordre n. Soit p un diviseur premier de n. Alors il existe un élément de G d'ordre p.

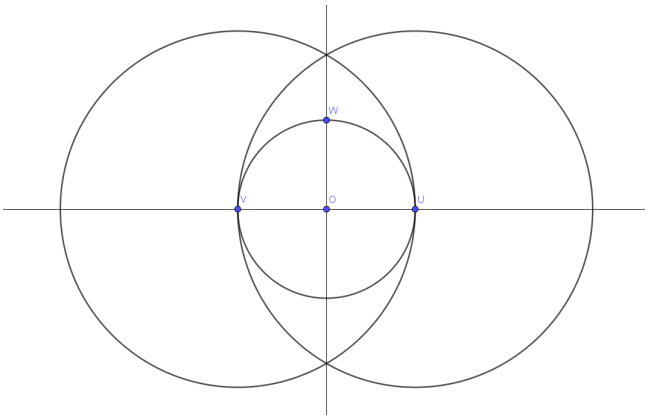


FIGURE 1 – Construction à la règle et au compas des éléments de $\mathbb{Z} \times \mathbb{Z}$.

1. Tracer un carré de même aire qu'un cercle de rayon 1 ?
2. Tracer un cube dont le volume est le double d'un cube dont l'arête est de longueur 1 ?
3. Diviser n'importe quel angle en trois parties égales ?

La première est plus connue sous le nom de quadrature du cercle et de nombreux mathématiciens ont cru réussir à construire un tel carré.

Bien que géométriques, ces questions sont en fait intimement liées à la théorie des corps. Soient O et U les deux points initiaux. Avec une règle on trace la droite d_1 passant par ces deux points. Cette droite définit notre axe x de telle manière que $O = (0, 0)$, $U = (1, 0)$. Avec un compas on peut construire le point $V = (-1, 0)$ en traçant un cercle centré en O et passant par U car le nouveau point d'intersection de ce cercle avec la droite d_1 est $(-1, 0)$ (voir FIGURE 1). Avec la même méthode on peut construire les points $(2, 0)$, $(-2, 0)$, $(3, 0)$, $(-3, 0)$ etc... Ensuite on trace le cercle C_1 centré en V passant par U et le cercle C_2 centré en U passant par V. On trace à la règle la droite d_2 passant par les points d'intersection de C_1 et C_2. Cette droite est perpendiculaire à d_1 et définit l'axe y. On trace le cercle C_3 centré en O et passant par U (ou V). L'intersection de C_3 avec d_2 est $W = (0, 1)$. Par la même logique que précédemment on peut construire les points $(0, -1)$, $(0, 2)$, $(0, -2)$ etc... mais aussi $(1, 1)$, $(3, 2)$, $(118, -3)$ etc... On montre ainsi que tous les points de $\mathbb{Z} \times \mathbb{Z}$ sont constructibles. Ce résultat n'est pas surprenant. On va montrer que l'ensemble des points constructibles de la forme $P = (a, 0)$ est un corps. Pour cela nous devons démontrer les lemmes suivants.

Lemme 3.90. *Soit d_1 une droite ne passant pas par le point constructible $A = (x, y)$ et soient B et C des points constructibles sur d_1. Alors on peut tracer une droite parallèle à d_1 passant par A avec la règle et le compas.*

Démonstration. (Voir FIGURE 2.) On trace un cercle C_1 centré en B et passant par A. Puis on trace la droite d_2 passant par A et B. Cette droite coupe C_1 en

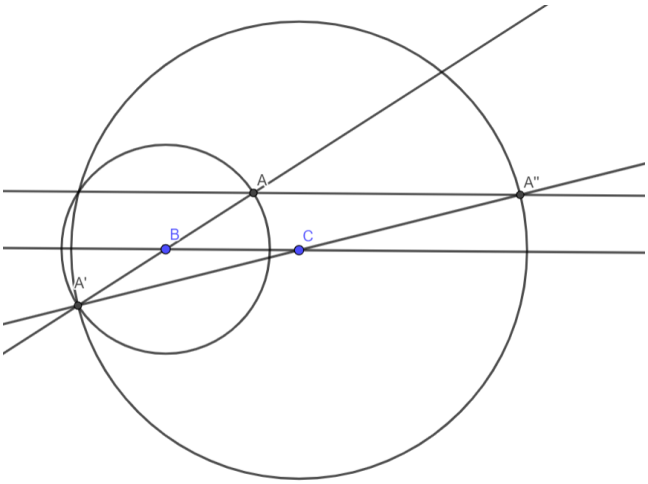


FIGURE 2 – Construction d'une droite parallèle à une autre, passant par un point donné.

un point A'. On trace le cercle C_2 centré en C et passant par A'. Puis on trace la droite d_3 passant par C et A'. Cette droite coupe C_2 en un nouveau point A''. On trace la droite d_4 passant par A et A''. Cette droite est parallèle à d_1 par le théorème des milieux car $\overline{CA'} = \overline{CA''}$ et $\overline{A'B} = \overline{BA}$ par construction. En particulier notons que A'' est aussi constructible et donc que la droite d_4 relie bien deux points constructibles. □

Lemme 3.91. *Le point $A = (a, b)$ est constructible si et seulement si $(a, 0)$ et $(b, 0)$ sont constructibles.*

Démonstration. Dans tous les cas, les axes x et y sont construits à partir des points $O = (0, 0)$, $U = (1, 0)$ et $W = (0, 1)$. Supposons que A est constructible. Alors par le lemme précédent, on peut construire une droite parallèle (passant par le point A et le point A'' constructible, construit dans le lemme précédent) à l'axe y dont l'intersection avec l'axe x est $(a, 0)$. Par conséquent, $(a, 0)$ est constructible. De même, on peut tracer une droite parallèle à l'axe x dont l'intersection avec l'axe y est $(0, b)$. On trace le cercle de centre O et passant par $(0, b)$. L'intersection $(b, 0)$ de ce cercle avec l'axe x est donc constructible. Inversément supposons que $(a, 0)$ et $(b, 0)$ sont constructibles. Alors $(0, b)$ est une des intersections du cercle centré en O et passant par $(b, 0)$ avec l'axe y. Par conséquent $(0, b)$ est constructible. Maintenant, comme expliqué dans l'introduction, on peut construire des droites perpendiculaires aux axes x et y passant par $(a, 0)$ et $(0, b)$ respectivement. L'intersection de ces deux droites est $A = (a, b)$ qui est donc constructible. □

Proposition 3.92. *L'ensemble des points constructibles de la forme $(a, 0)$ est un corps contenant $\mathbb{Q}$.*

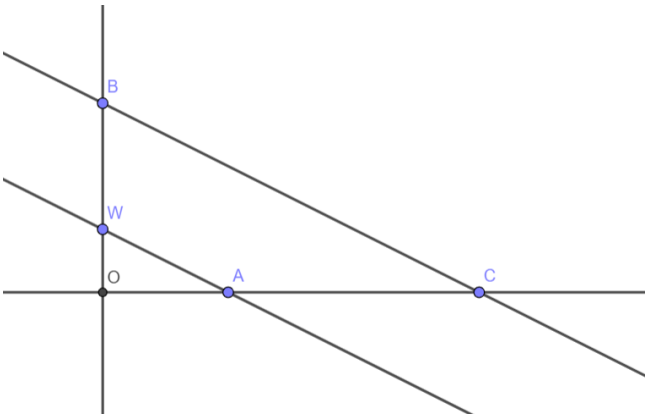


FIGURE 3 – Construction de $(ab, 0)$ et $(a/b, 0)$.

Démonstration. À nouveau, on a les points constructibles $O = (0, 0)$, $U = (1, 0)$ et $W = (0, 1)$. Si $(a, 0)$ et $(b, 0)$ sont constructibles, alors on montre que $(a+b, 0)$ est constructible. On trace la droite d_1 passant par $(a, 0)$ et W. Puis, on trace la droite d_2 parallèle à l'axe x et passant par W. Ensuite, on trace la droite perpendiculaire à $(b, 0)$. Son intersection avec d_2 est $(b, 1)$. Finalement, on trace la droite parallèle à d_1 passant par $(b, 1)$. Cette droite intersecte l'axe x en $(a + b, 0)$.

Ensuite on montre que $(ab, 0)$ est constructible. (Voir FIGURE 3.) On note $A = (a, 0)$ et $B(0, b)$. Le point B est bien entendu constructible car $(b, 0)$ l'est. On trace la droite d_1 reliant $W = (1, 0)$ et A. Puis on trace la droite parallèle à d_1 passant par B. Cette droite intersecte l'axe x en C. Comme les triangles COB et AOW sont semblables on sait que $\overline{CO}/\overline{AO} = \overline{BO}/\overline{WO}$ de sorte que $\overline{CO} = 1.b.a$. Par conséquent $C = (ab, 0)$.

Pour montrer que $\left(\frac{a}{b}, 0\right)$ est constructible il suffit d'interchanger les rôles de A et C dans la preuve précédente. □

Ceci montre que l'ensemble des nombres constructibles forme un corps. Il est clair que ce corps contient $\mathbb{Q}$. De plus, on se convainc assez facilement que si α est constructible alors $\sqrt{\alpha}$ est aussi constructible, le corps des nombres constructibles est une extension non triviale de $\mathbb{Q}$.

Comme on l'a vu, les constructions à la règle et au compas ne font intervenir que des droites et des cercles. Les points constructibles sont les points d'intersections entre des droites et des cercles à coefficients dans un certain corps $K \supseteq \mathbb{Q}$. Il est clair que le point d'intersection entre deux droites non parallèles à coefficients dans un corps K est un élément de $K \times K$. Maintenant, soit $ax+by+c = 0$ une droite à coefficients dans K et soit $x^2 + y^2 + dx + ey + f = 0$ un cercle, aussi à coefficients dans K. Il est clair que le nombre de points d'intersection entre cette droite et ce cercle est soit 0 soit 1 ou 2. Supposons qu'il existe au moins un point d'intersection. En isolant x dans l'équation de la droite et en

injectant son expression dans l'équation du cercle, on trouvera une équation de la forme $\alpha y^2 + \beta y + \gamma = 0$. Si α est nul alors $y \in K$ et donc $x \in K$ aussi. Supposons que $\alpha \neq 0$. Cette équation est à nouveau à coefficients dans K. Ses solutions sont clairement dans $K(\sqrt{\Delta})$ avec $\Delta = \beta^2 - 4\alpha\gamma$ et en injectant l'expression de y dans l'équation de la droite on trouve l'expression de x qui est aussi dans $K(\sqrt{\Delta})$. Par conséquent, les points d'intersection entre une droite et un cercle à coefficients dans K sont dans $K(\sqrt{\Delta}) \times K(\sqrt{\Delta})$. Il reste à étudier le cas de l'intersection entre deux cercles. Posons $C_1 \equiv x^2+y^2+dx+ey+f = 0$ et $C_2 \equiv x^2+y^2+ax+by+c = 0$ les équations des cercles à coefficients dans K. Encore une fois, il y a soit 0 intersections soit 1 ou 2. Supposons qu'il y a au moins un point d'intersection. Alors, en soustrayant l'équation de C_1 à celle de C_2 on a le système d'équations $x^2+y^2+dx+ey+f = 0$ et $(a-d)x+(b-e)y+(c-f) = 0$. Ceci revient à étudier l'intersection entre un cercle et une droite, chose qui a déjà été faite. Pour synthétiser, partant de points constructibles dans un corps K, les points d'intersections entre les cercles et les droites construits à partir de ces points sont des éléments de $K(\sqrt{\Delta}) \times K(\sqrt{\Delta})$.

Par la suite, nous dirons qu'un nombre α est constructible dans K pour signifier que $(\alpha, 0)$ est constructible.

Théorème 3.93. *(Théorème de Wantzel) Un nombre $\alpha \in \mathbb{R}$ est constructible si et seulement il existe une tour d'extension*

$$\mathbb{Q} = L_0 \subset L_1 \subset \cdots \subset L_n$$

avec $\alpha \in L_n$ et tel que $[L_{i+1} : L_i] \leq 2$ pour tout $0 \leq i \leq n-1$.

Démonstration. On part des points O et U de $\mathbb{Q} \times \mathbb{Q}$. Comme α est constructible, il existe une suite de construction à la règle et au compas tel que $(\alpha, 0)$ est le point d'intersection d'une droite avec un cercle ou d'une droite avec une droite ou d'un cercle avec un cercle à coefficients dans $K \times K$ pour un certain corps K. À la première étape, on construit un point à partir de droites et de cercles à coefficients dans $\mathbb{Q} = L_0$. On sait, par le paragraphe précédent, que les points d'intersections de ces droites et de ces cercles sont dans $\mathbb{Q}(\sqrt{a_1}) \times \mathbb{Q}(\sqrt{a_1})$ pour un certain $a_1 \in \mathbb{Q}$, de plus $[\mathbb{Q}(\sqrt{a_1}) : \mathbb{Q}] \leq 2$. On pose $L_1 = \mathbb{Q}(\sqrt{a_1})$. À l'étape m on construit le nouveau point d'intersection entre des droites et des cercles à coefficients dans un certain corps L_{m-1}. Le point d'intersection est dans $L_{m-1}(\sqrt{a_m}) \times L_{m-1}(\sqrt{a_m})$ pour un certain $a_m \in L_{m-1}$. De plus $[L_m(\sqrt{a_m}) : L_{m-1}] \leq 2$ et on pose $L_m = L_{m-1}(\sqrt{a_m})$. On construit ainsi une tour d'extension qui, à l'itération n, contient α. De plus la construction montre que $[L_{i+1} : L_i] \leq 2$ pour tout $0 \leq i \leq n-1$ d'où l'assertion.

Inversement, supposons qu'il existe une tour d'extension de la forme $\mathbb{Q} = L_0 \subset L_1 \subset \cdots \subset L_n$ tel que $\alpha \in L_n$ et $[L_{i+1} : L_i] \leq 2$ pour tout $0 \leq i \leq n-1$. Si $n = 0$ alors $\alpha \in \mathbb{Q}$ est constructible. Supposons que tous les éléments de L_m avec $m > 0$ sont constructibles. Comme $[L_{m+1} : L_m] \leq 2$ on sait qu'il existe $a \in L_m$ tel que $L_{m+1} = L_m(\sqrt{a})$. Or $\sqrt{a}$ est constructible donc L_{m+1} est un corps d'éléments constructibles. Par récurrence, cela montre que α est constructible. □

Proposition 3.94. *La quadrature du cercle est impossible.*

Démonstration. Soit C un cercle de rayon 1. Son aire vaut π et on se demande s'il est possible de tracer un carré dont l'aire est π. Ceci est équivalent à se demander si $\sqrt{\pi}$ est constructible. Or $\sqrt{\pi}$ n'est même pas algébrique, donc ne peut être contenu dans une tour d'extension de degré 2^n et cette construction est impossible. □

Proposition 3.95. *Il est impossible de tracer à la règle et au compas un cube de volume* 2*.*

Démonstration. Ceci revient à construire un cube dont l'arête est de longueur $2^{\frac{1}{3}}$. Or $[\mathbb{Q}(2^{\frac{1}{3}}) : \mathbb{Q}] = 3$ donc $2^{\frac{1}{3}}$ ne peut être contenu dans une extension de degré 2^n et cette construction est impossible. □

Proposition 3.96. *Un angle constructible θ est divisible en trois parties égales si et seulement si $4X^3 - 3X - \cos(\theta)$ est irréductible sur $\mathbb{Q}(\cos(\theta))$.*

Démonstration. On trace le cercle C_1 reliant centré en O et passant par U. Si θ est constructible, alors il existe une droite de pente θ dont le point d'intersection avec C_1 est $(\cos(\theta), \sin(\theta))$. Pour construire $\theta/3$, il nous faudrait construire le point $(\cos(\theta/3), \sin(\theta/3))$, c'est-à-dire pouvoir construire $\cos(\theta/3)$. Or $\cos(3u) = 4\cos(u)^3 - 3\cos(u)$ et en posant $3u = \theta$, $X = \cos(u)$ on a l'équation $f(X) = 4X^3 - 3X - \cos(\theta) = 0$. Si $f(X)$ est irréductible sur $\mathbb{Q}(\cos(\theta))$ alors $\cos(\theta/3)$, qui est une racine de ce dernier, est dans une extension de degré 3 sur $\mathbb{Q}$. Dans ce cas $\cos(\theta/3)$ n'est pas constructible et on ne peut diviser θ en trois parties égales. Sinon $f(X)$ n'est pas irréductible et il possède des facteurs de degré 1 et 2. Par conséquent, les extensions de $\cos(\theta)$ possédant $\cos(\theta/3)$ sont de degré 1 ou 2 et $\theta/3$ est constructible. □

Typiquement, il est impossible de diviser un angle de 60 degrés en 3 parties égales car $4X^3 - 3X - \cos(\pi/3) = 4X^3 - 3X - 1/2$ est irréductible sur $\mathbb{Q}$.

Pour l'instant, tous les problèmes ont étés résolus uniquement avec des extensions quadratiques. Une dernière grande question, résolue par Gauss, est de savoir quels sont les polygones réguliers constructibles à la règle et au compas. La démonstration nécessite l'utilisation des extensions cyclotomiques de $\mathbb{Q}$. La preuve peut être trouvée dans [22] (théorème 15.6) ou [32] (proposition 33.2).

Théorème 3.97. *Un polygone régulier à n côtés est constructible à la règle et au compas si et seulement si $\phi(n) = 2^n$ pour $n \geq 1$.*

4 Théorie de Galois infinie

Pour écrire ce chapitre nous nous basons sur les références [5],[7],[18],[21] (ch.7),[22] (ch.4),[23] (ch.4),[37] (ch.5 section 4).

4.1 Introduction

La théorie de Galois classique est restreinte à l'étude des extensions algébriques finies. Comme sous-entend son nom, la théorie de Galois infinie s'intéresse aux extensions algébriques de degré infini. Intuitivement, une extension galoisienne infinie est une union infinie d'extensions galoisiennes finies. De manière équivalente, une extension galoisienne infinie est le corps de décomposition d'une infinité de polynômes séparables. On peut par exemple penser à l'extension $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \ldots, \sqrt{p}, \ldots)$ où toutes les racines carrées de tous les nombres premiers sont adjointes à $\mathbb{Q}$. La grande question est de savoir si le théorème fondamental de la théorie de Galois fonctionne encore dans le cas des extensions infinies. La réponse est non, en ce sens que si L/K est une extension galoisienne infinie alors il existe, en général, plusieurs sous-groupes de $\mathrm{Gal}(L/K)$ qui fixent un même corps intermédiaire. Nous avons donc perdu la correspondance galoisienne. Il y a cependant une bonne nouvelle : il existe une topologie, dite de Krull, qui permet de rétablir la correspondance entre l'ensemble des corps intermédiaire entre L et K et l'ensemble des sous-groupes de $\mathrm{Gal}(L/K)$ qui sont **fermés** pour cette topologie. L'une des motivations de cette théorie est de comprendre le groupe de Galois absolu de $\mathbb{Q}$: $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ (ou plus généralement le groupe de Galois absolu de n'importe quel corps : $\mathrm{Gal}(\overline{K}/K)$). Ce groupe gigantesque contient tous les groupes de Galois $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ de toutes les extensions algébriques K de $\mathbb{Q}$ et chacun de ses quotients par un de ses sous-groupes normal est le groupe de Galois $\mathrm{Gal}(L/\mathbb{Q})$ d'une extension galoisienne L de $\mathbb{Q}$. Comprendre ce groupe c'est comprendre toute la structure des nombres algébriques. Aujourd'hui encore, ce groupe est mal compris et nous ne savons décrire essentiellement aucun de ses éléments.

4.2 Quelques rappels de topologie

Commençons par rappeler quelques caractérisations de la continuité d'une fonction.

Proposition 4.1. *Soient X et Y deux espaces topologiques. Soient $\mathcal{B}_X$, $\mathcal{S}_X$ et $\mathcal{B}_Y$, $\mathcal{S}_Y$ une base et une sous-base pour les espaces topologies X et Y respectivement. Alors une fonction $f : X \to Y$ est continue si et seulement si*

1. *Pour tout $x \in X$ et pour tout un ouvert V de Y contenant $f(x)$, il existe un ouvert U de X tel que $f(U) \subset V$.*
2. *L'image réciproque par f de tout ouvert de Y est un ouvert de X, i.e. $f^{-1}(U)$ est un ouvert de X pour tout ouvert U de Y.*
3. *L'image réciproque par f de tout ouvert de la base $\mathcal{B}_Y$ est un ouvert de X.*
4. *L'image réciproque par f de tout ouvert de la sous-base $\mathcal{S}_Y$ est un ouvert de X.*

Définition 4.1. Soit $(X_i)_{i\in I}$ un ensemble d'espaces topologiques et soit $X = \prod_{i\in I} X_i$ le produit cartésien des $(X_i)_{i\in I}$. La topologie produit sur X est la

topologie la moins fine telle que l'ensemble des projections $\pi_j : X \to X_j$ sont des fonctions continues.

Proposition 4.2. *Dans les notations de la définition précédente, une sous-base pour la topologie produit sur X est donnée par l'ensemble des*

$$S_j = \{\pi_j^{-1}(U_j) \mid j \in I \text{ et } U_j \text{ un ouvert de } X_j\}.$$

Nous aurons aussi besoin des notion suivantes.

Définition 4.2. Un espace topologique X est un espace de Hausdorff si pour tout $x, y \in X$ tels que $x \neq y$, il existe des ouverts $U_x \ni x$ et $U_y \ni y$ tels que $U_x \cap U_y = \emptyset$.

Définition 4.3. Un espace topologique est compact X si de tout recouvrement $X = \cup_{i\in I} U_i$ par des ouverts on peut extraire un sous-recouvrement fini $X = \cup_{i\in J} U_i$ (c'est-à-dire où $J \subseteq I$ est fini).

Pour la compacité, nous ne retiendrons que trois propriétés.

Proposition 4.3. *Un fermé dans un compact est compact.*

Proposition 4.4. *L'image d'un compact par une fonction continue est encore un compact.*

Théorème 4.5. *(Tychonoff) Soit $(X_i)_{i\in I}$ un ensemble d'espaces topologiques* ***compacts*** *et soit $X = \prod_{i\in I} X_i$ l'espace topologique muni de la topologie produit. Alors X est* ***compact****.*

Ce théorème s'applique même lorsque l'ensemble des indices I est infini.

Définition 4.4. Un espace topologique X est totalement discontinu si les seules composantes connexes de X sont les singletons.

Du reste, le lecteur est invité à consulter l'ouvrage [2] pour davantage de précisions.

4.3 Extensions algébriques infinies

Soit L/K une extension algébrique infinie. Par définition, chacun des éléments de L est algébrique sur K. Soit $\alpha \in L$. Alors, par définition, il existe un polynôme $f(X) \in K[X]$ tel que $f(\alpha) = 0$. Par conséquent il existe une extension de degré fini F/K telle que $\alpha \in F$. En fait, même si l'extension L/K est infinie, chacun de ses éléments est contenu dans une extension finie.

On dit toujours qu'une extension est galoisienne lorsque $\mathrm{Fix}(\mathrm{Gal}(L/K)) = K$ et où $\mathrm{Gal}(L/K)$ est toujours le groupe des automorphismes de L qui fixent K (dans le cas d'une extension infinie le groupe de Galois est lui aussi infini).

Proposition 4.6. *Soit L/K une extension galoisienne. Alors*

$$L = \bigcup L_i$$

où L_i parcourt l'ensemble des extensions galoisiennes finies de K contenues dans L.

Démonstration. Cela découle directement du paragraphe précédent. □

À nouveau, une extension est galoisienne si et seulement si elle est le corps de décomposition d'un ensemble de polynômes séparables (dans le cas d'une extension infinie, ça sera le corps de décomposition d'un ensemble infini de polynômes séparables.)

Remarque 4.7. On peut encore montrer que L/K est galoisienne si et seulement si L/K est normale et séparable. Au vu de ce qui précède, par les propositions 3.53, 3.54 et par le corollaire 3.63, on a encore que L/E est une extension galoisienne pour tout $K \subseteq E \subseteq L$. Au final, la seule différence avec le cas des extensions finies est que nous nous ne pouvons plus définir l'égalité $[L : K] = |\mathrm{Gal}(L/K)|$ dans le cas infini. Nous ne le démontrons pas, mais le théorème d'extensions des isomorphismes peut être étendu aux extensions de degré infini [7](voir par exemple [37]). De ce fait, l'homomorphisme $\mathrm{Gal}(L/K) \to \mathrm{Gal}(F/K)$, où $K \subseteq F \subseteq L$ est une extension galoisienne de degré fini, qui était une surjection dans le cas où L/K était une extension galoisienne de degré fini, l'est toujours dans le cas des extensions de degré infini. Comme le noyau de cette surjection est précisément $\mathrm{Gal}(L/F)$ on a, comme dans le cas fini, $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/F) \cong \mathrm{Gal}(F/K)$. Ce résultat est aussi vrai lorsque F/K n'est pas une extension galoisienne finie.

4.4 Topologie de Krull

Soit L/K une extension galoisienne et soit $\sigma \in \mathrm{Gal}(L/K)$. On va construire une topologie sur $\mathrm{Gal}(L/K)$ à partir des classes (à gauche) de $\mathrm{Gal}(L/K)$. Une base de voisinage de σ est donnée par

$$\sigma\mathrm{Gal}(L/F),$$

où F parcourt l'ensemble des extensions galoisiennes **finies** de K dans L. Pour un F fixé, $\sigma\mathrm{Gal}(L/F)$ est l'ensemble des automorphismes de L qui agissent comme σ sur F. Plus précisément, si $\tau \in \sigma\mathrm{Gal}(L/F)$ alors il existe $\theta \in \mathrm{Gal}(L/F)$ tel que $\tau = \sigma \circ \theta$. Ce faisant, $\tau(a) = \sigma(\theta(a)) = \sigma(a)$ pour tout $a \in F$ puisque θ fixe F. On a donc $\sigma|_F = \tau|_F$. Inversement, supposons que $\tau \in \mathrm{Gal}(L/K)$ et $\sigma|_F = \tau|_F$. Comme $\mathrm{Gal}(L/K)$ est un groupe il existe $\theta \in \mathrm{Gal}(L/K)$ tel que $\tau = \sigma \circ \theta$. Par hypothèse $\sigma(a) = \tau(a)$ pour tout $a \in F$, donc $\sigma(a) = \sigma(\theta(a))$ et, encore parce que $\mathrm{Gal}(L/K)$ est un groupe, $\theta(a) = a$. Mais alors $\theta|_F = \mathrm{id}$, donc $\theta \in \mathrm{Gal}(L/F)$. Par conséquent, $\tau = \sigma \circ \theta \in \sigma\mathrm{Gal}(L/F)$.

Plus l'extension F/K est de degré élevé (mais toujours de degré fini) plus $\sigma\mathrm{Gal}(L/F)$ est petit et plus ses éléments sont proches de σ.

Proposition 4.8. *Avec l'ensemble vide, l'ensemble des $\sigma Gal(L/F)$ où σ parcourt l'ensemble des éléments de $Gal(L/K)$ et où F parcourt l'ensemble des extensions galoisiennes finies de K dans L définissent une topologie sur $Gal(L/K)$. De manière équivalente, tout ouvert U de $Gal(L/K)$ est soit $\emptyset$ soit une union*

7. Cela nécessite le lemme de Zorn

de classes i.e. $U = \bigcup_{i\in I} \sigma_i Gal(L/F_i)$ *où les* F_i *sont des extensions galoisiennes finies de* K *dans* L*.*

Démonstration. Clairement $\mathrm{Gal}(L/K)(= \mathrm{id}\mathrm{Gal}(L/K))$ est un ouvert car K est une extension galoisienne finie de K. De même $\emptyset$ est l'ouvert trivial. Ensuite, l'union quelconque d'ouverts est encore un ouvert car les ouverts sont déjà définis comme des unions

$$U = \bigcup_{i\in I} \sigma_i \mathrm{Gal}(L/F_i).$$

Reste à voir qu'une intersection finie d'ouverts est un ouvert. Soit $U_1, \ldots, U_n$ un nombre fini d'ouverts et considérons leur intersection $U_1 \cap \cdots \cap U_n$. Si cette intersection est vide, il n'y a rien à montrer. Sinon, il existe au moins un élément $\sigma \in U_1 \cap \cdots \cap U_n$. On veut montrer qu'il existe un ouvert U contenant σ et qui est contenu dans l'intersection des U_i. Comme chaque U_i est un ouvert il existe une extension galoisienne F_i pour chaque U_i tel que $\sigma\mathrm{Gal}(L/F_i) \subset U_i$. Soit $F = F_1 \ldots F_n$ la composition de tous les F_i. C'est encore une extension finie de K et par construction $\sigma\mathrm{Gal}(L/F) \subset \sigma\mathrm{Gal}(L/F_i)$ pour chaque $1 \leq i \leq n$. Par conséquent $\sigma\mathrm{Gal}(L/F) \subset U_1 \cap \cdots \cap U_n$ et l'intersection des U_i est un ouvert. □

Définition 4.5. La topologie définie sur $\mathrm{Gal}(L/K)$ est appelée la topologie de **Krull**.

Si F/K est une extension galoisienne de degré fini, alors la topologie de Krull sur $\mathrm{Gal}(F/K)$ coïncide avec la topologie discrète. En effet, si F/K est fini alors $\sigma\mathrm{Gal}(K/K) = \{\sigma\}$ est un ouvert pour tout $\sigma \in \mathrm{Gal}(F/K)$. Par conséquent, tous les singletons de $\mathrm{Gal}(F/K)$ sont ouverts, ce qui montre bien que la topologie induite est la topologie discrète.

Définition 4.6. Un groupe topologique est un groupe G (ici multiplicatif) muni d'une topologie compatible avec les opérations du groupe. En d'autres termes, la multiplication

$$m : G \times G \to G : (x, y) \mapsto xy$$

et l'inversion

$$i : G \to G : x \mapsto x^{-1}$$

sont des fonctions continues au sens de la topologie sur G.

Proposition 4.9. *Muni de la topologie de Krull,* $Gal(L/K)$ *est un groupe topologique.*

Démonstration. Soit F une extension galoisienne finie de K dans L et soit $\sigma\tau\mathrm{Gal}(L/F)$ le voisinage associé de $\sigma\tau$. On va montrer que

$$m(\sigma\mathrm{Gal}(L/F) \times \tau\mathrm{Gal}(L/F)) \subset \sigma\tau\mathrm{Gal}(L/F),$$

la continuité de m en découlera. Soit θ, γ un élément de $\sigma\mathrm{Gal}(L/F) \times \tau\mathrm{Gal}(L/F)$. Par définition cela signifie que $\theta|_F = \sigma|_F$ et $\gamma|_F = \tau|_F$. Par conséquent $m((\theta, \gamma)) = \theta\gamma$ et si $a \in F$ alors $\gamma(a) = \tau(a) \in F$ donc $\theta(\gamma(a)) = \sigma(\tau(a))$ ou encore

$\theta\gamma \in \sigma\tau\mathrm{Gal}(L/F)$ d'où la continuité de m. Pour l'inversion, soit $\sigma^{-1}\mathrm{Gal}(L/F)$ le voisinage de σ^{-1} associé à F. On va montrer que

$$i(\sigma\mathrm{Gal}(L/F)) \subset \sigma^{-1}\mathrm{Gal}(L/F),$$

et comme précédemment, la continuité de i en découlera. Soit $\tau \in \sigma\mathrm{Gal}(L/F)$, c'est-à-dire un élément tel que $\tau|_F = \sigma|_F$. Alors $i(\tau) = \tau^{-1}$ et pour tout $a \in F$ on a $\tau^{-1}(a) = \sigma^{-1}(a)$ par ce qui précède. Par conséquent $\tau^{-1} \in \sigma^{-1}\mathrm{Gal}(L/F)$, d'où la conclusion. □

Reprenons L/K, une extension galoisienne infinie avec son groupe de Galois $\mathrm{Gal}(L/K)$ muni de la topologie de Krull. Considérons le produit

$$X = \prod_F \mathrm{Gal}(F/K)$$

où F parcourt l'ensemble des extensions galoisiennes finies de K dans L. Comme il a été vu précédemment, chacun des groupes finis $\mathrm{Gal}(F/K)$ est naturellement muni de la topologie discrète ce qui en fait des groupes topologiques. Nous pouvons donc munir X de la topologie produit et ce dernier hérite de la structure de groupe de ses facteurs en définissant la loi de composition interne composante par composante. Le produit X est, par conséquent, un groupe topologique. En outre, les groupes topologiques $\mathrm{Gal}(F/K)$ sont finis et discrets, donc compacts. Par le théorème de Tychonoff, cela montre que X est aussi compact. Pourquoi parlons-nous de ce produit ? Car le groupe topologique $\mathrm{Gal}(L/K)$ s'injecte naturellement dans X et que nous allons pouvoir déduire des propriétés de $\mathrm{Gal}(L/K)$ à partir des propriétés de X. Soit l'homomorphisme

$$f : \mathrm{Gal}(L/K) \to X = \prod_F \mathrm{Gal}(F/K) : \sigma \mapsto \prod_F \sigma|_F.$$

Cette fonction est injective, en effet $f(\sigma) = \prod_F \sigma|_F = \prod_F \mathrm{id}$ implique que $\sigma = \mathrm{id}$ sur tout L puisque L est l'union de toutes ses sous-extensions galoisiennes finies. Cela montre aussi que $\mathrm{Gal}(L/K) \cong \mathrm{Im}(f)$. On peut se convaincre de l'injectivité intuitivement. Le produit X n'est qu'un ensemble de groupes qu'on a "collé" les uns aux autres. Les composantes de X n'ont pas de liens entre elles alors que $\mathrm{Gal}(L/K)$ possède une structure plus restrictive : Si $F_1 \subset F_2$ sont des extensions galoisiennes finies de K dans L alors $(\sigma|_{F_2})|_{F_1} = \sigma|_{F_1}$ (la restriction de σ à F_2 doit coïncider avec la restriction de σ à F_1 lorsque ces deux automorphismes sont comparés sur le domaine F_1). Ces considérations vont nous amener à construire une expression plus précise de $\mathrm{Gal}(L/K) \cong \mathrm{Im}(f) \subset X$. Mais avant cela, montrons la proposition suivante.

Proposition 4.10. *Le groupe topologique Gal(L/K) est Hausdorff, totalement discontinu et compact.*

Démonstration. On suit [22] et [23].

Hausdorff : Soient $\sigma, \tau \in \mathrm{Gal}(L/K)$ deux automorphismes distincts. Il faut montrer qu'il existe deux voisinages disjoints V_1 et V_2 contenant σ et τ respectivement. Comme $\sigma \neq \tau$ il existe une extension galoisienne finie F/K telle que $\sigma|_F \neq \tau|_F$. Mais alors $\sigma\mathrm{Gal}(L/F) \cap \sigma\mathrm{Gal}(L/F) = \emptyset$, donc les voisinages $V_1 = \sigma\mathrm{Gal}(L/F)$ et $V_2 = \tau\mathrm{Gal}(L/F)$ conviennent.

Totalement discontinu : On doit montrer que les seuls parties connexes de $\mathrm{Gal}(L/K)$ sont les singletons. (Voir [7] pour la preuve.)

Compacité : L'idée est la suivante : On prouve que l'injection $f : \mathrm{Gal}(L/K) \to X$ définie précédemment est un homéomorphisme de $\mathrm{Gal}(L/K)$ dans $\mathrm{Im}(f)$. On montre ensuite que $\mathrm{Im}(f)$ est un fermé dans X. Comme un fermé dans un compact est compact, cela démontrera que l'image est compacte et comme l'image réciproque d'un compact par un homéomorphisme est aussi compact, cela achèvera la démonstration.

Pour que f soit un homéomorphisme de $\mathrm{Gal}(L/K)$ sur $\mathrm{Im}(f)$, il suffit de montrer que f et f^{-1} sont continues car on a déjà montré la bijectivité (en montrant l'injectivité). D'après la proposition 4.2, une sous-base pour la topologie produit est donnée par

$$S = \prod_{F \neq E} \mathrm{Gal}(F/K) \times \{\tau\},$$

où les F parcourent l'ensemble des extensions galoisiennes finies de K et $\tau \in \mathrm{Gal}(E/K)$. Maintenant, si $\sigma|_E = \tau$ alors $f^{-1}(S) = \sigma\mathrm{Gal}(L/E)$ qui est un ouvert de $\mathrm{Gal}(L/K)$. Par la proposition 4.1 partie 4), on en déduit que f est continue. Maintenant $f(\sigma\mathrm{Gal}(L/K)) = f(\mathrm{Gal}(L/K)) \cap S$ est un ouvert dans $\mathrm{Im}(f)$ donc f^{-1} est continue. Il en résulte que f est un homéomorphisme. Si $K \subseteq E_1 \subseteq E_2 \subset L$ et si $\sigma\mathrm{Gal}(L/K)$ alors en particulier $(\sigma|_{E_2})|_{E_1} = \sigma|_{E_1}$. Par conséquent, $\mathrm{Im}(f) = \bigcap_{E_2 \subseteq E_1} C_{E_2,E_1}$ où $C_{E_2,E_1} = \{\prod_F \sigma|_F$ tel que $(\sigma|_{E_2})|_{E_1} = \sigma|_{E_1}\} \subset X$. Or $C_{E_2,E_1} = \bigcup_{\sigma \in \mathrm{Gal}(E/K)}(\prod_{F \neq E_1,E_2} \mathrm{Gal}(E/K) \times R_\sigma \times \{\sigma\})$ où S_σ est l'ensemble des $\tau \in \mathrm{Gal}(E_2/K)$ tels que $\tau|_{E_1} = \sigma$. Comme la topologie sur les projections est la topologie discrète et que l'union est finie en en déduit que C_{E_2,E_1} est fermé. Mais l'intersection quelconque de fermés est encore un fermé, donc $\mathrm{Im}(f)$ est fermé dans X. Ceci achève la démonstration. □

Définition 4.7. Un groupe topologique qui est compact, Hausdorff et totalement discontinu est appelé un groupe **profini**.

Les groupes profinis possèdent la propriété de s'exprimer en terme de ce qu'on appelle une "limite **pro**jective de groupes topologiques **finis**" (d'où le nom profini). En fait si L/K est une extension galoisienne alors au vu de la démonstration précédente,

$$\mathrm{Gal}(L/K) = \{\prod(\sigma|_F) \in \prod \mathrm{Gal}(F/K) \mid (\sigma_{F_2})|_{F_1} = \sigma|_{F_1} \ \forall F_1 \subseteq F_2\} \subset X.$$

Dans notre contexte, on dit que l'ensemble des $\mathrm{Gal}(F/K)$ avec les projections $(\sigma_{F_2})|_{F_1} = \sigma|_{F_1} \forall F_1 \subseteq F_2$ forme un **système projectif**. La limite projective de

ce système projectif est par définition l'expression à droite de l'égalité ci-dessus. On la note

$$\mathrm{Gal}(L/K) = \varprojlim \mathrm{Gal}(F/K),$$

où F/K parcourt l'ensemble des extensions galoisiennes finies de K dans L. Tout groupe de Galois est un groupe profini, inversement on peut montrer que tout groupe profini est le groupe de Galois d'une extension galoisienne.

Proposition 4.11. *Soit $K \subseteq F \subseteq L$ une extension intermédiaire. Alors Gal(L/F) est fermé dans Gal(L/K).*

Démonstration. Soit $\sigma \notin \mathrm{Gal}(L/F)$ un élément de $\mathrm{Gal}(L/K)$. Alors il existe un $\alpha \in F$ tel que $\sigma(\alpha) \neq \alpha$. Comme $\alpha \in L$ il existe une extension galoisienne $K \subseteq E \subseteq L$ telle que $\sigma\mathrm{Gal}(L/E) \cap \mathrm{Gal}(L/F) = \emptyset$. Donc $\mathrm{Gal}(L/K) \setminus \mathrm{Gal}(L/F)$ est ouvert et $\mathrm{Gal}(L/F)$ est fermé. □

Proposition 4.12. *Soit H un sous-groupe de Gal(L/K). Alors la fermeture de H dans Gal(L/K) est $\overline{H}$ = Gal$(L/$Fix$(H))$. En d'autres termes, si H est fermé alors H = Gal$(L/$Fix$(H))$.*

Démonstration. On suit [7]. À priori $H \subseteq \mathrm{Gal}(L/\mathrm{Fix}(H))$. Par la proposition précédente $\mathrm{Gal}(L/\mathrm{Fix}(H))$ est fermé donc $\overline{H} \subseteq \mathrm{Gal}(L/\mathrm{Fix}(H))$. On montre que $\overline{H} \supseteq \mathrm{Gal}(L/\mathrm{Fix}(H))$. Soit $\sigma \in \mathrm{Gal}(L/K) \setminus \overline{H}$. On prouve que $\sigma \notin \mathrm{Gal}(L/\mathrm{Fix}(H))$. Comme $\overline{H}$ est fermé son complémentaire est ouvert et il existe un $K \subseteq E \subseteq L$ tel que E/K est finie, de sorte que $\sigma\mathrm{Gal}(L/E) \cap \overline{H} = \emptyset$. Supposons que pour tout $\alpha \in E$ on a que $\tau(\alpha) = \alpha$ pour tout $\tau \in H$ implique que $\sigma(\alpha) = \alpha$. On suppose donc que $\mathrm{Fix}(H_E) \subseteq \mathrm{Fix}(\sigma|_E)$. Comme $\mathrm{Gal}(E/K)$ est fini cela montre que $\sigma|_E \in \mathrm{Fix}(H_E)$ et il existe $\tau \in \mathrm{Fix}(H)$ tel que $\sigma|_E = \tau|_E$. Donc par définition $\tau \in \sigma\mathrm{Gal}(E/K)$. Mais ceci est impossible car on a choisi E tel que $\sigma\mathrm{Gal}(E/K) \cap \overline{H} = \emptyset$. Par conséquent il existe un $\alpha \in E$ tel que $\sigma(\alpha) \neq \alpha$ et $\tau(\alpha) = \alpha$ pour tout $\tau \in H$. Cela montre que $\sigma \notin \mathrm{Gal}(L/\mathrm{Fix}(H))$. □

Une conséquence directe de cette proposition est qui si H est fermé dans $\mathrm{Gal}(L/K)$ alors $H = \mathrm{Gal}(L/\mathrm{Fix}(H))$ ou encore $\mathrm{Fix}(H) = \mathrm{Fix}(\mathrm{Gal}(L/\mathrm{Fix}(H)))$, c'est-à-dire $L/\mathrm{Fix}(H)$ est une extension galoisienne.

Proposition 4.13. *Soit $K \subseteq F \subseteq L$ une extension intermédiaire* ***finie****. Alors Gal(L/F) est un sous-groupe ouvert de Gal(L/K). Inversement, tout sous-groupe ouvert de Gal(L/K) est de la forme Gal(L/F) pour F/K finie.*

Démonstration. Soit $\sigma \in \mathrm{Gal}(L/F)$. Notons E la clôture normale de F dans L. Alors $\sigma\mathrm{Gal}(L/E) \subseteq \mathrm{Gal}(L/F)$ et $\mathrm{Gal}(L/F)$ est ouvert. Inversement, si H est un sous-groupe ouvert de $\mathrm{Gal}(L/K)$ alors $H = \mathrm{Gal}(L/K) \setminus \bigcup_{\sigma \neq \mathrm{id}} \sigma H$, et H est le complémentaire d'une union d'ouverts. Donc H est fermé. Par la proposition 4.12 on a donc que $H = \mathrm{Gal}(L/F)$ où $F = \mathrm{Fix}(H)$. Maintenant $\mathrm{Gal}(L/K) = \bigcup_\sigma \sigma\mathrm{Gal}(L/F)$ (union disjointe) et comme $\mathrm{Gal}(L/K)$ est compact on peut extraire un sous-ensemble fini $S \subseteq \mathrm{Gal}(L/K)$ tel que $\mathrm{Gal}(L/K) = \bigcup_{\sigma \in S} \sigma\mathrm{Gal}(L/F)$. Par conséquent $|\mathrm{Gal}(L/K) : \mathrm{Gal}(L/F)| < +\infty$ et F/K est une extension finie. □

Il existe cependant des sous-groupes de $\mathrm{Gal}(L/K)$ d'indice fini mais qui ne sont pas ouverts [8](voir [21] ch. 7). En combinant ces propositions, on a enfin le fameux théorème de la théorie de Galois infinie.

Théorème 4.14. *(Théorème fondamental de la théorie de Galois infinie) Soit L/K une extension galoisienne. Notons $\overline{\mathcal{G}}$ l'ensemble des sous-groupes fermés de $Gal(L/K)$ et $\mathcal{F}$ l'ensemble des extensions intermédiaires de L/K. Alors la fonction $\Gamma : \overline{\mathcal{G}} \to \mathcal{F} : H \mapsto Fix(H)$ est une bijection et son inverse est donnée par $\Omega : F \mapsto Gal(L/F)$. De plus, F est une extension finie de K si et seulement si $Gal(L/F)$ est un sous-groupe ouvert dans $Gal(L/K)$.*

Démonstration. Soit H un sous-groupe fermé de $\mathrm{Gal}(L/K)$. On sait par la proposition 4.12 que $H = \mathrm{Gal}(L/\mathrm{Fix}(H))$, donc

$$\Gamma(H) = \mathrm{Fix}(H) = \mathrm{Fix}(\mathrm{Gal}(L/\mathrm{Fix}(H))).$$

Si $K \subseteq E \subseteq L$ alors $\Omega(E) = \mathrm{Gal}(L/E)$ est un sous-groupe fermé de $\mathrm{Gal}(L/K)$ par la proposition 4.11. Donc

$$\mathrm{Fix}(\mathrm{Gal}(L/E)) = E,$$

par la proposition 4.12 (ou aussi parce que L/E est une extension galoisienne). En combinant les deux résultats on a

$$\Omega(\Gamma(H)) = \Omega(\mathrm{Fix}(H)) = \mathrm{Gal}(L/\mathrm{Fix}(H)) = H,$$

par conséquent Γ et Ω sont bien inverses l'une de l'autre. □

4.5 Application aux extensions cyclotomiques

4.5.1 Construction de $\mathbf{Gal}(\mathbb{Q}(\zeta_{3^\infty})/\mathbb{Q})$

Maintenant que nous avons vu la théorie, nous voudrions construire le groupe de Galois d'une extension galoisienne infinie. Un choix à la fois non trivial et raisonnable est le cas des extensions cyclotomiques. Nous avons vu au chapitre précédent que si ζ_n est une racine primitive n-ième de l'unité alors $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ est une extension galoisienne de degré $\varphi(n)$ et son groupe de Galois est $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. Prenons un exemple concret en considérant le cas où $n = 3$. L'objectif est de calculer le groupe de Galois de la plus petite extension de $\mathbb{Q}$ qui possède toutes les racines 3-ièmes, 3^2-ièmes, 3^3-ièmes etc... de l'unité jusqu'à l'infini. Cette extension est notée $\mathbb{Q}(\zeta_{3^\infty})$. Par construction, c'est le corps de décomposition de l'ensemble des polynômes de la forme $X^{3^n} - 1$ pour $n \geq 1$. Cette extension s'écrit aussi comme l'union des extensions cyclotomiques (donc galoisiennes) finies $\mathbb{Q}(\zeta_{3^\infty}) = \bigcup_{i \geq 1} \mathbb{Q}(\zeta_{3^i})$. Par ce qui a été vu précédemment, on sait que

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{3^\infty})/\mathbb{Q}) \cong \varprojlim (\mathbb{Z}/3^n\mathbb{Z})^\times = \mathbb{Z}_3^\times,$$

8. Il faut à nouveau utiliser le lemme de Zorn.

qui est, par définition, le groupe des entiers 3-adiques inversibles (voir [12] pour plus d'information sur les nombres p-adiques). Ce groupe est l'ensemble des séries formelles $\sum_{i=0}^{+\infty} a_i 3^i$ telles que $a_0 \neq 0$ et $a_i \in \mathbb{Z}/3\mathbb{Z}$ pour tout $i \geq 1$. Essayons de comprendre ce que cela veut dire, nous verrons par la même occasion comment $(\mathbb{Z}/3^n\mathbb{Z})^\times$ forme un système projectif. Partons d'un élément de $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{3^\infty})/\mathbb{Q})$ et étudions son action sur ζ_3. Comme $\sigma(\zeta_3) = \sigma|_{\mathbb{Q}(\zeta_3)}(\zeta_3)$, la restriction de σ à $\mathbb{Q}(\zeta_3)$ est un élément τ_1 de $\mathrm{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q})$. Or, comme il a été vu, τ_1 envoie une racine primitive 3-ième de l'unité sur une de ses puissances (qui est encore une racine primitive 3-ième de l'unité) données par les éléments du groupe $(\mathbb{Z}/3\mathbb{Z})^\times$. Par conséquent, il existe $n_1 \in (\mathbb{Z}/3\mathbb{Z})^\times = \{1, 2\}$ tel que $\sigma(\zeta_3) = \tau_1(\zeta_3) = \zeta_3^{n_1}$. Considérons maintenant l'action de σ sur ζ_{3^2}. Par le même raisonnement que précédemment, σ se restreint à un élément τ_2 de $\mathrm{Gal}(\mathbb{Q}(\zeta_{3^2})/\mathbb{Q})$. Un tel élément envoie ζ_{3^2} sur une de ses puissances, il existe donc $n_2 \in (\mathbb{Z}/3^2\mathbb{Z})^\times = \{1, 2, 4, 5, 7, 8\}$ de sorte que $\sigma(\zeta_{3^2}) = \tau_2(\zeta_{3^2}) = \zeta_{3^2}^{n_2}$. Maintenant $\zeta_{3^2}^3 = \zeta_3$ donc

$$\sigma(\zeta_{3^2}^3) = \tau_2(\zeta_{3^2})^3 = \zeta_{3^2}^{3n_2} = \zeta_3^{n_2},$$

mais aussi

$$\sigma(\zeta_{3^2}^3) = \sigma(\zeta_3) = \tau_1(\zeta_3) = \zeta_3^{n_1},$$

d'où $\zeta_3^{n_1} = \zeta_3^{n_2}$, c'est-à-dire $n_2 \equiv n_1 \bmod 3$ puisque $\zeta_3^3 = 1$. Ainsi, pour $n_1 = 1$ on a $n_2 = 1$ ou $n_2 = 4$ ou $n_2 = 7$ et si $n_1 = 2$ alors $n_2 = 2$ ou $n_2 = 5$ ou $n_2 = 8$ et ces valeurs dépondront de σ. Considérons maintenant le cas plus général où σ agit sur une racine primitive 3^m-ième de l'unité et une racine primitive 3^{m+1}-ième de l'unité pour $m \geq 1$ quelconque. Alors

$$\sigma(\zeta_{3^{m+1}}^3) = \sigma(\zeta_{3^m}) = \zeta_{3^m}^{n_m},$$

où $n_m \in \mathbb{Z}/3^m\mathbb{Z} \cong \mathrm{Gal}(\mathbb{Q}(\zeta_{3^m})/\mathbb{Q})$, mais aussi

$$\sigma(\zeta_{3^{m+1}}^3) = \sigma(\zeta_{3^{m+1}})^3 = \zeta_{3^m}^{n_{m+1}},$$

où $n_{m+1} \in \mathbb{Z}/3^{m+1}\mathbb{Z} \cong \mathrm{Gal}(\mathbb{Q}(\zeta_{3^{m+1}})/\mathbb{Q})$. Par conséquent $\zeta_{3^m}^{n_m} = \zeta_{3^m}^{n_{m+1}}$ d'où $n_{m+1} \equiv n_m \bmod 3^m$ (et non pas mod 3) car $\zeta_{3^m}^{3^m} = 1$. Par récurrence, nous voyons que la relation $n_{m+1} \equiv n_m \bmod 3^n$ pour tout $m \geq 1$ signifie que

$$\begin{aligned}
n_1 &= a_0, \\
n_2 &= n_1 + 3a_1 = a_0 + 3a_1, \\
n_3 &= n_2 + 3^2 a_2 = a_0 + 3a_1 + 3^2 a_2, \\
&\cdots \\
n_m &= \sum_{i=0}^{m-1} a_i 3^i,
\end{aligned}$$

où les a_i sont choisis dans $\mathbb{Z}/3\mathbb{Z}$ pour tout $0 \leq i \leq m-1$ et $a_0 \neq 0$ (On pourrait choisir d'autres représentants pour les a_i mais cela nous compliquerait

la vie. Notre choix produit bien une représentation unique de chacun des n_i). En prenant la limite à l'infini on a $n := \sum_{i=0}^{+\infty} a_i 3^i$ (qu'il faut regarder comme une série formelle i.e. il ne faut pas véritablement sommer les termes) avec $a_0 \neq 0$ et $\sigma(\zeta) = \zeta^n$ pour toute racine primitive 3^n-ième de l'unité $\zeta \in \mathbb{Q}(\zeta_{3^\infty})$. En prenant par exemple ζ_{3^2} nous avons

$$\sigma(\zeta_{3^2}) = \zeta_{3^2}^n = \zeta_{3^2}^{\sum_{i=0}^{+\infty} a_i 3^i} = \zeta_{3^2}^{a_0+3a_1} = \zeta_{3^2}^{n_2},$$

car $\zeta_{3^2}^{3^2} = 1$ de sorte que tous les autres termes de la série peuvent être ignorés. En résumé, σ détermine tous les a_i de la série définie par n et la série définie par n défini l'automorphisme σ. Il est important de voir que les automorphismes de $\mathrm{Gal}(\mathbb{Q}(\zeta_{3^\infty})/\mathbb{Q})$ possèdent une forme bien déterminée induite par les équivalences modulo 3^n.

4.5.2 Construction de deux sous-groupes fixant le même corps

Cet exemple permet aussi de montrer que la topologie de Krull définie sur $\mathrm{Gal}(\mathbb{Q}(\zeta_{3^\infty})/\mathbb{Q})$ est bel est bien utile. Pour ce faire, on construit deux sous-groupes de $\mathrm{Gal}(\mathbb{Q}(\zeta_{3^\infty})/\mathbb{Q})$ qui fixent le même corps. Cela montrera que la correspondance galoisienne ne fonctionne pas sans la topologie de Krull. Considérons les automorphismes $\sigma, \tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_{3^\infty})/\mathbb{Q})$ tels que $\sigma(\zeta_{3^n}) = \zeta_{3^n}^4$ et $\tau(\zeta_{3^n}) = \zeta_{3^n}^7$ pour tout $n \geq 1$. Ces automorphismes génèrent des sous-groupes cycliques $\langle\sigma\rangle$ et $\langle\tau\rangle$ dans $\mathrm{Gal}(\mathbb{Q}(\zeta_{3^\infty})/\mathbb{Q})$. Rappelons le fait suivant.

Lemme 4.15. *(Notation multiplicative) Pour que deux groupes cycliques infinis $\langle x\rangle = \{x^m \mid m \in \mathbb{Z}\}$ et $\langle y\rangle = \{x^m \mid m \in \mathbb{Z}\}$ soient égaux il faut et il suffit que $x = y$ ou $x = y^{-1}$.*

Démonstration. Il est évident que si $x = y$ ou $x = y^{-1}$ alors $\langle x\rangle = \langle y\rangle$ puisque les puissances négatives sont autorisées. Inversement, supposons que $\langle x\rangle = \langle y\rangle$. Alors il existe $n, m \in \mathbb{Z}$ tels que $x = y^n$ et $y = x^m$. Par conséquent, $x = y^n = x^{nm}$ et comme $\langle x\rangle$ est de cardinal infini, $x \neq x^j$ pour tout $j \in \mathbb{Z} \setminus \{0\}$, c'est-à-dire $x = x^{nm}$ si et seulement si $nm = 1$. Cela montre que $n = 1$ et $m = 1$ ou $n = -1$ et $m = -1$, d'où le lemme. □

Grâce à ce lemme, on montre que $\langle\sigma\rangle$ et $\langle\tau\rangle$ sont des sous-groupes distincts. En effet, si ces deux sous-groupes étaient égaux alors on aurait $\sigma = \tau$ ou $\sigma = \tau^{-1}$. Mais $\sigma(\zeta_{3^n}) = \tau(\zeta_{3^n})$ implique que $\zeta_{3^n}^4 = \zeta_{3^n}^7$ et $\sigma(\zeta_{3^n}) = \tau^{-1}(\zeta_{3^n})$ implique que $\zeta_{3^n}^4 = \zeta_{3^n}^{7^{-1}}$ pour tout $n \geq 1$. Pour le premier cas, cela implique que $4 \equiv 7 \bmod 3^n$ pour tout $n \geq 1$, ce qui est faux à partir de $n = 2$. Pour le second cas, il nous faut savoir que $7^{-1} = (1 + 2.3)^{-1}$ possède une expression en terme de série

$\sum_{i=0}^{+\infty} a_i 3^i$ dans $\mathbb{Z}_3^\times$. En fait,

$$\begin{aligned}\frac{1}{7} &= -\frac{104}{1-3^6} \\ &= \left(1+3+2.3^3+3^4+2\sum_{n=5}^{+\infty}3^n\right)\left(\sum_{n=0}^{+\infty}3^{6n}\right) \\ &= 1+3+2.3^3+3^4+2.3^5+\dots\end{aligned}$$

et la condition $\zeta_{3^n}^4 = \zeta_{3^n}^{7^{-1}}$ pour tout $n \geq 1$ se réécrit

$$4 \equiv 7^{-1} \equiv 1+3+2.3^3+3^4+2.3^5+\dots \bmod 3^n,$$

qui est fausse à partir de $n = 4$. Tout ceci montre que $\langle\sigma\rangle \neq \langle\tau\rangle$. Cependant, on prouve que $\mathrm{Fix}(\langle\sigma\rangle) = \mathrm{Fix}(\langle\tau\rangle) = \mathbb{Q}(\zeta_3)$. Notons déjà que $\sigma(\zeta_3) = \zeta_3^4 = \zeta_3$ et $\tau(\zeta_7) = \zeta_3^7 = \zeta_3$ donc que $\mathbb{Q}(\zeta_3) \subseteq \mathrm{Fix}(\langle\sigma\rangle)$ et $\mathbb{Q}(\zeta_3) \subseteq \mathrm{Fix}(\langle\tau\rangle)$. Maintenant, pour tout $n \geq 1$, les automorphismes $\sigma|_{\mathbb{Q}(\zeta_{3^n})} := \sigma_n$ et $\tau|_{\mathbb{Q}(\zeta_{3^n})} := \tau_n$ génèrent des sous-groupes cycliques $\langle\sigma_n\rangle$ et $\langle\tau_n\rangle$ de $\mathrm{Gal}(\mathbb{Q}(\zeta_{3^n})/\mathbb{Q}) \cong (\mathbb{Z}/3^n\mathbb{Z})^\times$. En tant que sous-groupes de $(\mathbb{Z}/3^n\mathbb{Z})^\times$ ceux-ci sont de la forme

$$\langle\sigma_n\rangle \cong \{4^m \bmod 3^n \mid m \geq 0\}$$

et

$$\langle\tau_n\rangle \cong \{7^m \bmod 3^n \mid m \geq 0\}.$$

L'ordre (le cardinal) de $\langle\sigma_n\rangle$ est égal au plus petit entier m tel que $4^m \equiv 1 \bmod 3^n$. Par la théorie des groupes, nous savons aussi que l'ordre de tout sous-groupe de $(\mathbb{Z}/3^n\mathbb{Z})$ est un diviseur de l'ordre de ce groupe, et nous savons que $\mathrm{Card}((\mathbb{Z}/3^n\mathbb{Z})) = \varphi(3^n) = 2.3^{n-1}$ donc $m = 2$ ou $m|3^{n-1}$.

Lemme 4.16. *L'ordre de $\langle\sigma_n\rangle$ est égal à 3^{n-1}.*

Démonstration. Au vu du paragraphe ci-dessus, il s'agit de montrer que

$$4^{3^{n-1}} \equiv 1 \bmod 3^n$$

et

$$4^{3^{n-2}} \not\equiv 1 \bmod 3^n$$

pour tout $n \geq 2$. Par la formule du binôme de Newton on a

$$\begin{aligned}4^{3^{n-1}} &= (1+3)^{3^{n-1}} \\ &= \sum_{k=0}^{3^{n-1}} \frac{(3^{n-1})!}{(k!)(3^{n-1}-k)!}3^k.\end{aligned}$$

Il nous faut donc étudier le nombre de fois que 3 divise $C_{3^{n-1}}^k = \frac{(3^{n-1})!}{(k!)(3^{n-1}-k)!}$. Pour $k = 0$ il est clair que $C_{3^{n-1}}^0 = 1$. Pour $k \geq 1$ nous utilisons la fonction [9]

9. Cette fonction s'appelle la valuation p-adique.

$v_p(n)$ qui désigne le nombre de fois qu'un entier n est divisible par le nombre premier p. On vérifie tout de suite que $v_p(x/y) = v_p(x) - v_p(y)$ et $v_p(xy) = v_p(x) + v_p(y)$ pour tout $x, y \in \mathbb{Z}$ non nuls. Par la formule de Legendre,

$$v_3(n!) = \sum_{i=1}^{+\infty} \left\lfloor \frac{n}{3^i} \right\rfloor,$$

où $\lfloor x \rfloor$ désigne la partie entière de x. En appliquant cette formule à $(3^{n-1})!$ on trouve

$$v_3((3^{n-1})!) = 3^{n-2} + 3^{n-2} + \cdots + 3 + 1 = \frac{1 - 3^{n-1}}{1 - 3}.$$

Ensuite $v_3((k!)(3^{n-1} - k)!) = v_3(k!) + v_3((3^{n-1} - k)!)$ et par la formule de Legendre

$$v_3((k!)(3^{n-1} - k)!) = \sum_{i=0}^{+\infty} \left\lfloor \frac{k}{3^i} \right\rfloor + \left\lfloor \frac{3^{n-1} - k}{3^i} \right\rfloor.$$

Mais la fonction "floor" vérifie les propriétés suivantes : $\lfloor x + n \rfloor = \lfloor x \rfloor + n$ et aussi $\lfloor -n \rfloor = -\lfloor n \rfloor$ pour tout $n \in \mathbb{Z}$ et pour tout $x \in \mathbb{R}$. De plus si $x \in \mathbb{R} \setminus \mathbb{Z}$ alors $\lfloor -x \rfloor = -1 - \lfloor x \rfloor$ (Exemple $\lfloor 3.2 \rfloor = -4 = -1 - \lfloor 3 \rfloor$). Par conséquent

$$\begin{aligned}
\sum_{i=0}^{+\infty} \left\lfloor \frac{k}{3^i} \right\rfloor + \left\lfloor \frac{(3^{n-1} - k)}{3^i} \right\rfloor &= \sum_{i=0}^{v_3(k)} 3^{n-1-i} + \sum_{i=v_3(k)+1}^{n-1} \left(3^{n-1-i} - 1 \right) \\
&= n - 1 - (v_3(k) + 1) + 1 + \sum_{i=0}^{n-1} 3^{n-1-i} \\
&= n - 1 - v_3(k) + \frac{1 - 3^{n-1}}{1 - 3}.
\end{aligned}$$

En combinant tous les résultats on a

$$\begin{aligned}
v_3(C^k_{3^{n-1}}) &= v_3\left(\frac{(3^{n-1})!}{(k!)(3^{n-1} - k)!} \right) \\
&= v_3((3^{n-1})!) - v_3((k!)(3^{n-1} - k)!) \\
&= n - 1 - v_3(k).
\end{aligned}$$

Dès lors, $n - 1 - v_3(k)$ est le nombre de fois que $C^k_{3^{n-1}}$ est divisible par 3. Cela montre aussi que $C^k_{3^{n-1}} 3^k$ est divisible $n - 1 - v_3(k) + k$ fois par 3. Mais $v_3(k) < k$ pour tout $k \geq 1$, du coups $n - 1 - v_3(k) + k \geq n$ et

$$4^{3^{n-1}} \equiv 1 + \sum_{k=1}^{3^n - 1} C^k_{3^{n-1}} 3^k \equiv 1 \bmod 3^n.$$

Reste à montrer que $4^{3^{n-2}} \not\equiv 1 \bmod 3^n$, ce qui revient à montrer que

$$4^{3^{n-1}} \not\equiv 1 \bmod 3^{n+1}$$

pour tout $n \geq 1$. On a toujours $v_3(C^k_{3^{n-1}}) = n-1-v_3(k)$ et $C^0_{3^{n-1}} = 1$. Pour $k=1$, $v_3(C^1_{3^{n-1}}) = n-1-v_3(1) = n-1$ donc $v_3(C^1_{3^{n-1}}3^1) = n$. Pour $k>1$ alors $v_3(C^k_{3^{n-1}}3^k) = n-1-v_3(k)+k$ et $v_3(k)+2 \leq k$ d'où $v_3(C^k_{3^{n-1}}3^k) \geq n+1$ et

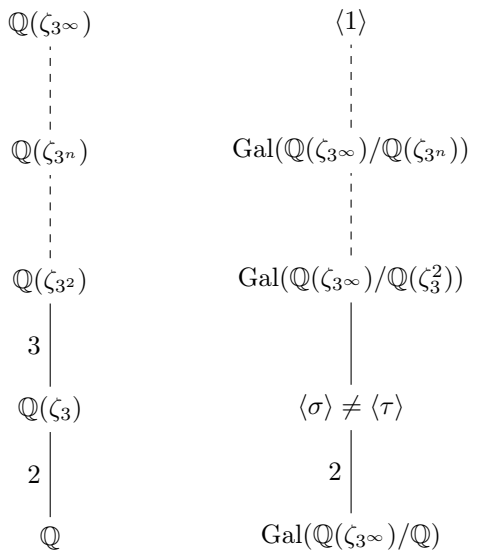
$$4^{3^{n-1}} \equiv 1+3^n \not\equiv 1 \bmod 3^{n+1}.$$

□

Définition 4.8. Soit G un groupe d'ordre $p^n u$ où p est un nombre premier, u n'est pas divisible par p et $n \geq 1$. Un p-sous-groupe de Sylow est un sous-groupe d'ordre p^n.

Les théorèmes de Sylow montrent que, dans les conditions de la définition, un tel sous-groupe existe toujours. De plus, si H et N sont deux p-sous-groupes de Sylow alors ils sont conjugués.

Dans notre cas, le groupe $(\mathbb{Z}/p^n\mathbb{Z})^\times$ est d'ordre $p^{n-1}(p-1)$ et le sous-groupe $\langle\sigma_n\rangle$ est un p-sous-groupe de Sylow pour ce groupe puisque son ordre est p^{n-1} par le lemme précédent. En outre, en suivant les mêmes étapes que la démonstration du lemme précédent, on montre que le sous-groupe $\langle\tau_n\rangle$ est aussi d'ordre p^{n-1} (la seule différence étant que $7 = 1+2.3$ et le "2" ne joue aucun rôle dans le nombre de fois que les coefficients binômiaux sont divisibles par 3.). Comme $(\mathbb{Z}/3^n\mathbb{Z})^\times$ est un groupe cyclique, il est, en particulier, abélien. Par conséquent, des sous-groupes conjugués dans $(\mathbb{Z}/3^n\mathbb{Z})^\times$ sont en fait égaux. Par les théorèmes de Sylow, cela montre que $\langle\sigma_n\rangle = \langle\tau_n\rangle$. Par le théorème fondamental de la théorie de Galois, l'indice des sous-groupes $\langle\sigma_n\rangle$ et $\langle\tau_n\rangle$ dans $(\mathbb{Z}/3^n\mathbb{Z})^\times$ désigne le degré de l'extension fixée par ces sous-groupes. Comme cet indice est par définition $\mathrm{Card}((\mathbb{Z}/3^n\mathbb{Z})^\times)/\mathrm{Card}(\langle\sigma_n\rangle) = \frac{3^{n-1}(3-1)}{3^{n-1}} = 2$ on en déduit que $[\mathrm{Fix}(\langle\sigma_n\rangle) : \mathbb{Q}] = 2$. Or, nous avons vu précédemment que le corps fixé par $\langle\sigma\rangle$ contient au moins $\mathbb{Q}(\zeta_3)$ qui est de degré 2. Par conséquent, $\mathbb{Q}(\zeta_3) = \mathrm{Fix}(\langle\sigma_n\rangle) = \mathrm{Fix}(\langle\tau_n\rangle)$ pour tout $n \geq 1$. Mais comme $\mathbb{Q}(\zeta_{3^\infty}) = \bigcup_{n\geq 1}\mathbb{Q}(\zeta_{3^n})$ on en conclut que $\mathbb{Q}(\zeta_3) = \mathrm{Fix}(\langle\sigma\rangle) = \mathrm{Fix}(\langle\tau\rangle)$ et nous avons enfin montré qu'il existe deux sous-groupes de $\mathrm{Gal}(\mathbb{Q}(\zeta_{3^\infty})/\mathbb{Q})$ qui fixent un même corps, $\mathbb{Q}(\zeta_3)$ en l'occurrence. Par le théorème X cela signifie qu'au moins un des deux sous-groupes $\langle\sigma\rangle$ ou $\langle\tau\rangle$ n'est pas fermé. On peut montrer que leur fermeture est le groupe multiplicatif $1+3\mathbb{Z}_3$ (et on a $\mathbb{Z}_3^\times/(1+3\mathbb{Z}_3) \cong (\mathbb{Z}/3\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q})$).



4.5.3 Construction de l'extension $\mathbb{Q}(\zeta_\infty)$

Tout ce qui a été construit précédemment est facilement généralisable à l'extension $\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}$ où ζ_p est une racine primitive p-ième de l'unité. Sans surprise, son groupe de Galois est

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}) \cong \varprojlim (\mathbb{Z}/p^n\mathbb{Z})^\times = \mathbb{Z}_p^\times,$$

et les éléments du groupes multiplicatifs $\mathbb{Z}_p^\times$ sont les séries formelles $\sum_{i=0}^{+\infty} a_i p^i$ où $a_i \in \{0, 1, \ldots, p-1\}$ avec $a_0 \neq 0$. On peut aller encore plus loin et construire le corps contenant toutes les racines n-ièmes de l'unité. On note $\mathbb{Q}(\zeta_\infty)$ l'extension de $\mathbb{Q}$ qui contient les racines 2-ièmes, 3-ièmes,4-ièmes etc... jusqu'à l'infini. Cette extension est le corps de décomposition de l'ensemble des polynômes de la forme $X^n - 1$ pour tout $n \geq 1$. C'est aussi l'union $\mathbb{Q}(\zeta_\infty) = \cup_{i \geq 1} \mathbb{Q}(\zeta_n)$. Son groupe de Galois est

$$\mathrm{Gal}(\mathbb{Q}(\zeta_\infty)/\mathbb{Q}) \cong \varprojlim (\mathbb{Z}/n\mathbb{Z})^\times = \widehat{\mathbb{Z}}^\times,$$

et on peut montrer que $\widehat{\mathbb{Z}}^\times = \prod_p \mathbb{Z}_p^\times$ où le produit est pris sur l'ensemble des nombre premiers p. Par le théorème de Kronecker-Weber ([36]), l'extension $\mathbb{Q}(\zeta_\infty)/\mathbb{Q}$ contient toutes les extensions abéliennes de $\mathbb{Q}$. Le groupe $\widehat{\mathbb{Z}}^\times$ étant lui-même abélien, $\mathbb{Q}(\zeta_\infty)/\mathbb{Q}$ est la plus grande extension abélienne de $\mathbb{Q}$. Au delà de cette extension, les groupes de Galois fixant $\mathbb{Q}$ associés ne sont plus abéliens. Malgré que ce groupe soit infiniment plus grand que $\mathrm{Gal}(\mathbb{Q}(\zeta_{3^\infty})/\mathbb{Q})$, il est en fait encore infiniment plus petit que le groupe de Galois absolu $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

4.5.4 Deux mots sur la théoire de Galois inverse

Terminons en mentionnant qu'une autre approche pour étudier le groupe $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ est d'étudier ses quotients. Cela revient à se demander quels sont les groupes qui peuvent être le groupe de Galois d'une extension galoisienne finie de $\mathbb{Q}$. Cette question est (entre autres) l'objet de la théorie de Galois inverse. La conjecture est que tout groupe fini est le groupe de Galois d'une extension finie de $\mathbb{Q}$. En particulier, tous les groupes de la forme $(\mathbb{Z}/n\mathbb{Z})^\times$ vérifient cette propriété grâce à ce que nous avons démontré sur les extensions cyclotomiques. Par le théorème de Chafarevitch ([29]), tout groupe résoluble vérifie aussi cette propriété. Le théorème de Feit-Thompson montre que les groupes finis d'ordre impair sont résolubles ([4],[24]). Cela donne une idée du genre de groupes qui peuvent être des groupes de Galois (sur $\mathbb{Q}$). On trouvera davantage d'informations sur cette théorie dans les références [17], [20],[21],[35].

5 Théorie de Galois en théorie algébrique des nombres

Ce chapitre s'inspire de [1],[23], [28],[30].

5.1 Introduction

L'objectif de ce chapitre est de montrer l'influence du groupe de Galois sur la décomposition des idéaux premiers de l'anneau des entiers d'un corps de nombres dans une extension galoisienne finie de ce dernier. Pour cela, nous rappelons les notions d'éléments irréductibles, premiers, d'unités et d'idéaux premiers ainsi que les théorèmes concernant la factorisation des idéaux en idéaux premiers. Cette théorie fait partie de la théorie algébrique des nombres et certains auteurs l'appellent la théorie de ramification de Hilbert. Une des applications historique de l'étude de la factorisation des idéaux et la preuve de Ernst Kummer (1810-1893) d'un cas particulier du dernier théorème de Fermat.

5.2 Éléments premiers et éléments irréductibles

Avant de commencer, rappelons les concepts de base. Soit A un anneau intègre, commutatif et unitaire.

Définition 5.1. On appelle unité tout élément $u \in A$ inversible pour la multiplication.

Example 5.1. Les unités de $\mathbb{Z}$ sont -1 et 1. Si A est un corps alors les unités sont $A^* = \{x \in A \mid x \neq 0\}$. Les unités de $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ sont ± 1 et $\pm i$.

Proposition 5.2. *L'ensemble de unités de A forme un groupe pour la multiplication.*

Démonstration. Si u, v sont des unités alors il existe u^{-1} et v^{-1} dans A de sorte que $(uv)(v^{-1}u^{-1}) = 1$ et uv est encore inversible. Le produit est associatif et, par définition, si u est une unité u^{-1} aussi. □

Définition 5.2. Deux éléments $a, b \in A$ sont dits associés s'il existe une unité u tel que $a = ub$.

Si a, b sont associés on note $a \sim b$.

Définition 5.3. Un élément non nul et non inversible $x \in A$ est dit irréductible si $x = ab$ pour $a, b \in A$ implique que a ou b est une unité dans A.

Définition 5.4. Un élément non nul et non inversible $x \in A$ est dit premier si $x|ab$ implique que $x|a$ ou $x|b$.

Remarque 5.3. Les éléments premiers de l'anneau des entiers $\mathbb{Z}$ coïncident avec ses éléments irréductibles. Dans ce cas, ce sont les bien connus nombres premiers. En effet, soit $p \in \mathbb{Z}$ un nombre premier, si $p = ab$ avec $a, b \in \mathbb{Z}$ alors clairement a ou b est 1 ou -1, donc tout nombre premier est irréductible. Pour montrer que tout nombre premier est un élément premier (donc vérifiant $p|ab \implies p|a$ ou $p|b$) il suffit de voir que si $p|ab$ mais que $p \nmid b$ alors, par l'identité de Bézout, il existe $x, y \in \mathbb{Z}$ tels que

$$xp + yb = 1.$$

En multipliant des deux côtés de l'égalité par a il résulte que $xpa + yba = a$. Or $p|p$, $p|ab$ donc $p|a$.

Ce qui précède est tout à fait remarquable.

Example 5.4. Considérons par exemple l'anneau

$$\mathbb{Z} + i\sqrt{7}\mathbb{Z} = \{a + i\sqrt{7}b \mid a, b \in \mathbb{Z}\}.$$

Alors l'élément 2 est irréductible car

$$2 = (a + \sqrt{7}ib)(c + \sqrt{7}id)$$

implique que

$$4 = (a^2 + 7b^2)(c^2 + 7d^2).$$

Or cela signifie que $a^2 + 7b^2 = 1$ ou 2 ou 4. Si $a^2 + 7b^2 = 1$ alors $a = \pm 1$ et $b = 0$, si $a^2 + 7b^2 = 2$ il n'y a pas de solution et si $a^2 + 7b^2 = 4$ alors $a = \pm 2$ et $b = 0$. Dans le premier cas $a + \sqrt{7}ib = \pm 1$ qui est clairement une unité dans $\mathbb{Z} + \sqrt{7}i\mathbb{Z}$. Sinon $a + \sqrt{7}ib = \pm 2$ et

$$(a + \sqrt{7}ib)(c + \sqrt{7}id) = \pm 2(c + \sqrt{7}id) = 2$$

d'où $c + \sqrt{7}id = \pm 1$ est une unité. En conclusion, 2 est irréductible. Cependant 2 n'est pas un élément premier. En effet, 2 divise $(1 + \sqrt{7}i)(1 - \sqrt{7}i) = 8$ mais 2 ne divise aucun de ces facteurs car il n'existe pas $a, b \in \mathbb{Z} + \sqrt{7}i\mathbb{Z}$ tel que $2(a + b\sqrt{7}i) = (1 + \sqrt{7}i)$ ou $2(a + b\sqrt{7}i) = (1 - \sqrt{7}i)$.

Proposition 5.5. *Si $p \in A$ est un élément premier alors il est irréductible.*

Démonstration. Supposons que $p = ab$ pour $a, b \in A$. Dès lors $p|ab$ et, comme p est un élément premier, $p|a$ ou $p|b$. Sans perte de généralité supposons que $p|a$. Alors $1 = (\frac{a}{p})b$ et on conclut que b est un élément inversible, donc une unité. Par conséquent p est irréductible. □

En général nous n'avons pas la réciproque ; tout élément irréductible n'est pas premier. Le fait que ces deux ensembles coïncident pour l'anneau $\mathbb{Z}$ vient de ce qu'il est, en particulier, principal.

Proposition 5.6. *Si A est un anneau intègre principal alors ses éléments premiers coïncident avec ses éléments irréductibles.*

Démonstration. Par la propriété précédente, il suffit de montrer que tout élément irréductible est premier. Soit $p \in A$ un élément irréductible tel que $p|ab$ pour $a, b \in A$. Sans perte de généralité, supposons que $p \nmid a$, alors l'idéal $\langle p, a\rangle = \{xp + ya \mid x, y \in A\} \neq \langle p\rangle$. Comme A est principal il existe $b \in A$ tel que $\langle b\rangle = \langle p, a\rangle$ et b divise a et p. Si $b|p$ alors, par l'irréductibilité de p, il existe une unité $u \in A$ tel que $ub = p$ et $p \sim b$. Or $b|a$ donc il existe $c \in A$ tel que $bc = a$ et $u^{-1}pc = a$ donc $p|a$ ce qui contredit l'hypothèse $p \nmid a$. La seule possibilité est que b est une unité. Il existe alors $d \in A$ tel que $bd = 1$. En outre $b \in \langle p, a\rangle$ donc il existe $x, y \in A$ tel que $b = xp + ya$ ou encore $b = db^2 = dxpb + dyab$ mais alors $p|dxpb$, $p|dyab$ donc $p|b$. Ceci montre la primalité de p car $p|ab$ implique que $p|a$ ou $p|b$. □

Les anneaux principaux forment un cas particulier d'une classe d'anneaux plus généraux appelés anneaux factoriels [10]. Dans ces derniers, éléments premiers et irréductibles coïncident toujours et comme dans $\mathbb{Z}$ il existe une factorisation unique de chaque élément en terme d'éléments irréductibles et d'unités.

Définition 5.5. Un anneau F est factoriel si, pour tout élément non nul et non inversible x, il existe nombre fini d'éléments irréductibles $p_1, p_2 \ldots, p_n \in F$ tel que

$$x = p_1 p_2 \ldots p_n,$$

où $p_1, p_2 \ldots, p_n$ sont uniques à unité près.

Example 5.7. On peut montrer que l'anneau $\mathbb{Z} + \sqrt{5}i\mathbb{Z}$ n'est pas factoriel. En effet, 3 est irréductible car $3 = (a + b\sqrt{5}i)(c + d\sqrt{5}i)$ implique que $a^2 + 5b^2 = 1$ ou 3. Si $a^2 + 5b^2 = 1$ alors $a = \pm 1$ et $b = 0$ donc $a + b\sqrt{5}i = \pm 1$ est une unité. Si $a^2 + 5b^2 = 3$ il n'y a pas de solutions donc 3 est irréductible. On montre de la même manière que 43 est irréductible. Or

$$129 = 3.43 = (2 + 5\sqrt{5}i)(2 - 5\sqrt{5}i),$$

10. Les anglais distinguent "unique factorization domain" et "factorization domain". Le premier signifie que la décomposition en éléments irréductibles est unique, le second pas. Le terme "domain" peut signifier anneau commutatif unitaire ou anneau commutatif unitaire intègre selon le contexte.

et les éléments $(2+5\sqrt{5}i)$ et $(2-5\sqrt{5}i)$ sont irréductibles car $2+5\sqrt{5}i = (a+b\sqrt{5}i)(c+d\sqrt{5}i)$ implique que $a^2+5b^2 = 129$ ou 43 ou 3 ou 1. Pour 43 et 3 il n'y a pas de solutions. Pour 1 cela implique que $a+b\sqrt{5}i$ est une unité et dans ce cas, que $2+5\sqrt{5}i$ est irréductible. Si $a^2+5b^2 = 129$ alors $a = \pm 7$ et $b = \pm 4$ ou $a = \pm 2$ et $b = \pm 5$. Dans le second cas on conclut que $2+5\sqrt{5}i$ est irréductible facilement. Dans le premier cas il suffit de développer $(a+b\sqrt{5}i)(c+d\sqrt{5}i) = 2+\sqrt{5}i$ en remplaçant a et b par leurs valeurs pour se rendre compte qu'il n'y a pas de solutions. Finalement, il reste à montrer que 3 et 43 ne sont pas associés à $2+5\sqrt{5}i$ et $2-5\sqrt{5}i$. Or $(2\pm\sqrt{5}i)/3$ et $(2\pm\sqrt{5}i)/43$ ne sont pas dans $\mathbb{Z}+\sqrt{5}i\mathbb{Z}$. Dès lors 129 admet deux factorisations différentes dans $\mathbb{Z}+\sqrt{5}i\mathbb{Z}$.

Pour terminer cette introduction, il faut remarquer que les éléments irréductibles d'un anneau peuvent ne plus être irréductibles dans une de leurs extensions. En effet, considérons l'anneau des entiers $\mathbb{Z}$ et son extension $\mathbb{Z}[i]$. L'élément 5 est irréductible dans $\mathbb{Z}$ mais

$$5 = (1+2i)(1-2i)$$

dans $\mathbb{Z}[i]$. On a vu dans l'exemple 5.1 que les seules unités de $\mathbb{Z}[i]$ sont ± 1 et $\pm i$. Donc 5 se factorise en éléments non inversibles et n'est plus irréductible dans cette extension.

L'objectif de la prochaine section est de "sauver" l'unicité de la factorisation en éléments irréductibles en généralisant les notions d'éléments irréductibles et d'éléments premiers. La bonne manière de généraliser ces notions est de considérer les idéaux premiers dans des anneaux dits de Dedekind (ce que sont les anneaux des entiers des extensions finies de $\mathbb{Q}$). Dans ces derniers, idéaux premiers et idéaux maximaux coïncident de la même manière que les éléments irréductibles et les éléments premiers d'un anneau factoriels coïncident. Les sections suivantes aborderont le lien entre la théorie de Galois et la factorisation de ces idéaux premiers dans des extensions galoisiennes finies $K/\mathbb{Q}$. En deux mots, si $p\mathbb{Z}$ est un idéal premier de $\mathbb{Z}$ alors ce dernier ne sera pas nécessairement un idéal premier dans l'anneau des entiers de l'extension de $\mathbb{Q}$. Il possèdera donc une factorisation de la forme $pO_K = \mathfrak{p}_1^{e_1}\dots\mathfrak{p}_n^{e_n}$ (dans le cas d'une extension galoisienne tous les e_i sont égaux) où O_K est l'anneau des entiers de K (jouant le même rôle que $\mathbb{Z}$ dans $\mathbb{Q}$ pour K) et où les $e_i \geq 1$. Si l'on regarde la manière dont $p\mathbb{Z}$ se factorise dans les extensions intermédiaires de $K/\mathbb{Q}$ on a alors qu'il existe une plus petite extension $E/\mathbb{Q}$ telle que $pO_E = \mathfrak{p}_1\dots\mathfrak{p}_n$ avec $[O_E/\mathfrak{p}_i : \mathbb{Z}/p\mathbb{Z}] := 1$ ($O_E/\mathfrak{p}_i$ est un corps car $\mathfrak{p}$ est un idéal maximal). C'est dans cette extension que $p\mathbb{Z}$ rencontre tous les facteurs qui seront présents dans sa factorisation dans K. Ensuite il y a une extension F/E dans K telle que $pO_F = \mathfrak{p}_1\dots\mathfrak{p}_n$ (comme dans E) mais avec $[O_F/\mathfrak{p}_i : \mathbb{Z}/p\mathbb{Z}] = [O_K/\mathfrak{p}_i : \mathbb{Z}/p\mathbb{Z}]$. Enfin il y a la dernière extension K/F dans laquelle $p\mathbb{Z}$ "se ramifie". C'est dans cette dernière partie que les e_i apparaissent dans la factorisation de $p\mathbb{Z}$. Par le théorème fondamental de la théorie de Galois, ces extensions successives correspondent à des sous-groupes particuliers de $\mathrm{Gal}(K/\mathbb{Q})$. On peut donc dire que

le groupe de Galois régit le lien entre l'arithmétique dans $\mathbb{Q}$ et l'arithmétique dans K.

La notation des idéaux dans le paragraphe précédent est usuelle dans cette théorie. Nous l'utiliserons uniquement dans le cadre de ce chapitre.

5.3 Anneau des entiers d'un corps de nombre

Définition 5.6. Un corps de nombres est une extension finie de $\mathbb{Q}$.

Définition 5.7. Soit K un corps de nombres. Un élément $x \in K$ est appelé entier algébrique s'il existe un polynôme monique $f(X)$ à coefficients dans $\mathbb{Z}$ tel que $f(x) = 0$.

Example 5.8. Le nombre $\sqrt{2}$ est un entier algébrique car il est racine de $f(X) = X^2 - 2$. Au contraire $\frac{5-i\sqrt{23}}{8}$ n'est pas un entier algébrique car son polynôme minimal est $x^2 - \frac{5}{4}x + \frac{3}{4}$.

La première propriété que nous voulons démontrer est que l'ensemble des entiers algébriques de K forme un anneau intègre $O_K \subset K$. La définition suivante est une généralisation de ce concept à des anneaux quelconques.

Définition 5.8. Soient A et B deux anneaux intègres tel que $A \subseteq B$ et soit $b \in B$. On dit que b est entier sur A s'il existe un polynôme monique $f(X) \in A[X]$ tel que $f(b) = 0$.

Nous allons démontrer un certain nombre de propriétés que vérifient ces entiers et nous transposerons ces résultats au cas particulier des corps de nombres.

Proposition 5.9. *Soient $A \subseteq B \subseteq C$ des anneaux intègres. Si $c \in C$ est entier sur A alors c est entier sur B.*

Démonstration. Si c est entier sur A alors il existe un polynôme monique $f(X) \in A[X]$ tel que $f(c) = 0$. Comme $A \subseteq B$, $f(X) \in B[X]$ et c est entier sur B. □

Là où les corps et les extensions de corps s'écrivent naturellement en termes d'espaces vectoriels, les anneaux (et plus tard les idéaux) s'écrivent plus naturellement en terme de modules.

Définition 5.9. Soit A un anneau. Un A-module (à gauche) M est un groupe abélien additif muni d'une opération de multiplication de $A \times M$ dans M tel que pour tout $a, b \in A$ et pour tout $x, y \in M$ on a

- $1.x = x$
- $(ab).x = a.(b.x)$
- $(a + b).x = a.x + b.x$
- $a.(x + y) = a.x + a.y$.

La "taille" d'un K-espace vectoriel est la dimension de cet espace vectoriel sur K. Chez les modules on parle plutôt de rang. Il n'est pas dit qu'un A-module possède une base sur A. Lorsque le module en possède une, on dit que ce module est libre et son rang est donné par le nombre d'éléments dans cette base.

Proposition 5.10. *Soient $A \subseteq B$ deux anneaux intègres. Les éléments $b_1, \ldots, b_n \in B$ sont entiers sur A si et seulement si $A[b_1, \ldots, b_n]$ est un A-module de type fini.*

Démonstration. On suit [1] (théorème 4.1.3) et [23] (proposition 2.2). La preuve se fait par récurrence. Supposons que $n = 1$. Si $b = b_1$ est entier sur A alors il existe un polynôme $f(x) = x^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in A[X]$ tel que

$$f(b) = b^n + a_{n-1}b^{n-1} + \cdots + a_1b + a_0 = 0.$$

Donc

$$b^n \in Ab^{n-1} + Ab^{n-2} + \cdots + Ab + A,$$

et par récurrence, pour tout $m \geq 0$

$$b^m \in Ab^{n-1} + Ab^{n-2} + \cdots + Ab + A.$$

Par conséquent, $A[b] = Ab^{n-1} + Ab^{n-2} + \cdots + Ab + A$ est un A-module de type fini. Supposons maintenant que la proposition est vraie pour $n = m > 1$. Supposons que $C = A[b_1, \ldots, b_{m-1}]$ est un A-module de type fini. Comme C est un anneau dans B et que $b_m \in \{b_1, \ldots, b_n\}$ est entier sur A, par la proposition 5.9 b_m est entier sur C. Par le premier pas de récurrence, cela montre que $C[b_m]$ est un C-module de type fini sur C. Par conséquent $C[b_m]$ est un A-module de fini.

Inversément supposons que $A[b]$ est un A-module de type fini et de rang n. Alors il existe $\omega_1, \ldots \omega_n \in A[b]$ tel que

$$A[b] = A\omega_1 + \cdots + A\omega_n.$$

En particulier, comme $b\omega_i \in A[b]$ pour tout $1 \leq i \leq n$, il existe un matrice $(a)_{ij} \in A^{n \times n}$ tel que $b\omega = A\omega$ où $\omega = (\omega_1 \ldots \omega_n)^t$. L'équation matricielle se réécrit

$$(A - bI)\omega = 0.$$

Comme $\omega \neq 0$ et que l'équation possède une solution il faut que $\det(A - bI) = 0$. Or, cela signifie que b est racine du polynôme caractéristique de A. Donc b est entier sur A. □

Corollaire 5.11. *Soient $A \subseteq B$ deux anneaux intègres. L'ensemble des éléments entiers sur A forme un anneau $\overline{A} \subseteq B$.*

Démonstration. Soient $b_1, b_2 \in B$ deux éléments entiers sur A. Alors $A[b_1, b_2]$ est un A-module de type fini. En outre $b_1 + b_2, b_1b_2, b_1 - b_2 \in A[b_1, b_2]$. Par conséquent $A \subseteq A[b] \subseteq A[b_1, b_2]$ où $b = b_1 + b_2$ ou $b = b_1b_2$ ou $b = b_1 - b_2$, donc le A-module $A[b]$ est de type fini sur A et $b_1b_2, b_1 + b_2, b_1 - b_2$ sont entiers sur A. □

L'anneau $\overline{A}$ du corollaire est appelé la **fermeture intégrale** de A dans B. On dit que B est entier sur A si tout élément de B est entier sur A, c'est-à-dire si $\overline{A} = B$.

Proposition 5.12. *Soient $A \subseteq B \subseteq C$ des anneaux intègres. Si C est entier sur B et B est entier sur A alors C est entier sur A.*

Démonstration. Soit $c \in C$ un élément non nul. Comme C est entier sur C il existe un polynôme $f(X) = \sum_{i=0}^{n} b_i X^i \in B[X]$ avec $b_n = 1$ tel que $f(c) = 0$. Considérons le A-module $A[b_1, \ldots, b_n]$. C'est un A-module de type fini sur A car B est entier sur A. De plus, $A[b_1, \ldots, b_n, c]$ est un $A[b_1, \ldots, b_n]$-module de type fini car c est élément entier sur $A[b_1, \ldots, b_n]$. Par conséquent $A[b_1, \ldots, b_n, c]$ est un A-module de type fini et comme c est arbitraire cela montre que C est entier sur A. □

Nous nous intéressons maintenant aux anneaux des entiers de $\mathbb{Q}$ et de ses extensions.

Définition 5.10. La fermeture intégrale de $\mathbb{Z}$ dans $\mathbb{C}$ est notée $\mathbb{A}$. C'est l'anneau des entiers algébriques de $\mathbb{C}$.

Définition 5.11. Soit K un corps de nombre. L'anneau $O_K = \mathbb{A} \cap K$ est appelé l'anneau des entiers de K. C'est l'ensemble des entiers algébriques dans K. De manière équivalente, O_K est la fermeture intégrale de $\mathbb{Z}$ dans K.

Maintenant soit L/K une extension finie et soit $O_L = \mathbb{A} \cap L$ l' anneaux des entiers de L. Alors la fermeture intégrale de O_K dans L est O_L. En effet, notons C la fermeture intégrale de O_K dans L. On a $\mathbb{Z} \subseteq O_K \subseteq C$ où O_K est entier sur $\mathbb{Z}$ et C est entier sur O_K. Par la proposition 5.12 cela montre que C est entier sur $\mathbb{Z}$, donc $C \subseteq O_L$. Ensuite O_L étant entier sur $\mathbb{Z}$, il est entier sur O_K par la proposition 5.9. Par conséquent, $O_L \subseteq C$ et $O_L = C$ par ce qui précède.

Proposition 5.13. *L'anneau des entiers O_K d'un corps de nombre K est intègre.*

Démonstration. Cela vient du fait que $O_K \subset K$ et que K est un corps, donc intègre. □

Comme O_K est intègre, on peut considérer son corps des fractions.

Proposition 5.14. *Le corps des fractions de l'anneau des entiers O_K est K.*

Démonstration. Comme K est un corps, si $a, b \in O_K$ avec $b \neq 0$ alors $a/b \in K$ et $\mathrm{Frac}(O_K) \subseteq K$. Soit $\alpha \in K$. Comme K est une extension finie de $\mathbb{Q}$ il existe un polynôme $a_0, \ldots a_{n-1} \in \mathbb{Q}$ tel que

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$$

dans K. Soit $b \in \mathbb{N}$ le plus petit commun multiple des dénominateurs des a_i. On a, en multipliant par b^n,

$$(b\alpha)^n + ba_{n-1}\alpha^{n-1} + \cdots + b^{n-1}a_1(b\alpha) + b^n a_0 = 0,$$

avec $b^n a_i \in \mathbb{Z}$ pour $0 \leq i \leq n-1$. Par conséquent $c = b\alpha$ est un entier algébrique (puisqu'il est la racine d'un polynôme monique à coefficient dans $\mathbb{Z}$). Cela montre que $\alpha = c/b$ est le quotient d'un élément $b \in \mathbb{Z} \subseteq O_K$ et d'un élément $c \in \mathbb{Z} \cap K = O_K$. Par conséquent, $\mathrm{Frac}(O_K) = K$. □

Définition 5.12. Soit A un anneau intègre et F son corps des fractions. La fermeture intégrale de A dans F est appelée la clôture intégrale de A. On dit que A est intégralement clos s'il coïncide avec sa clôture intégrale.

Théorème 5.15. *Soit K un corps de nombres, O_K son anneau des entiers. Alors O_K est intégralement clos.*

Démonstration. Soit $a \in K$ un élément entier sur O_K. On montre que $a \in O_K$. Comme a est entier sur O_K et que O_K est entier sur $\mathbb{Z}$ on sait par la propriété 5.12 que a est entier sur $\mathbb{Z}$. Mais alors $a \in \mathbb{A} \cap K = O_K$ d'où la conclusion. □

Définition 5.13. Soit $K/\mathbb{Q}$ une extension galoisienne de degré n. Le discriminant d d'un ensemble d'éléments $\alpha_1, \ldots, \alpha_n$ est défini comme

$$d(\alpha_1, \ldots, \alpha_n) = \det(\sigma_i(\alpha_j)),$$

$1 \leq i, j \leq n$ et où σ_i parcourt l'ensemble des éléments de $\mathrm{Gal}(K/\mathbb{Q})$.

On peut montrer [11] que dans la configuration de la définition précédente, le discriminant est toujours un nombre rationnel. On appelle discriminant de K le discriminant d'une base.

Définition 5.14. Soient $\omega_1, \ldots, \omega_n \in K$ formant une base pour un idéal $\mathfrak{a} \subset O_K$. On appelle discriminant de $\mathfrak{a}$ l'élément $d(\mathfrak{a}) = d(\omega_1, \ldots, \omega_n)$. Si ces éléments forment une base pour K alors $d(K) = d(\omega_1, \ldots, \omega_n)$ est le discriminant de K.

De plus, il existe toujours des $\omega_1, \ldots, \omega_n \in \mathfrak{a}$ tels que $d(\mathfrak{a}) \neq 0$. En fait, le choix de la base n'influence pas la valeur de $d(\mathfrak{a})$ ou $d(K)$.

Proposition 5.16. *Soit $K/\mathbb{Q}$ une extension de degré n. Soit $\mathfrak{a}$ un idéal non nul de O_K. Alors $\mathfrak{a}$ est un $\mathbb{Z}$-module libre de rang n.*

Démonstration. On suit [1] (par exemple). Comme $\mathfrak{a}$ est non nul il existe $\omega_1, \ldots, \omega_n \in \mathfrak{a}$ tel que

$$d(\omega_1, \ldots, \omega_n) \neq 0.$$

En outre $d(\omega_1, \ldots, \omega_n) \in \mathbb{Z}$. Par conséquent, l'ensemble

$$\{|d(\omega_1, \ldots, \omega_n)| \mid \omega_1, \ldots, \omega_n \in \mathfrak{a} \text{ tel que } d(\omega_1, \ldots, \omega_n) \neq 0\}$$

admet un élément minimal dans $\mathbb{Z}$. Soit $d(\omega_1, \ldots, \omega_n)$ cet élément dont la valeur absolue est minimal. Comme $d(\omega_1, \ldots, \omega_n) \neq 0$, les éléments $\omega_1, \ldots, \omega_n$ forment une base du $\mathbb{Q}$-espace vectoriel K. En particulier, tout élément de $a \in \mathfrak{a}$ peut s'écrire comme une combinaison linéaire

$$a = \alpha_1\omega_1 + \cdots + \alpha_n\omega_n,$$

avec $\alpha_1, \ldots, \alpha_n \in \mathbb{Q}$. Supposons maintenant que l'un des α_i n'est pas dans $\mathbb{Z}$. Sans perte de généralité on peut supposer que $\alpha_1 \notin \mathbb{Z}$. Dans ce cas, il existe un

11. Nous ne le ferons pas.

entier m tel que $m < \alpha_1 < m+1$. Posons $\gamma = a - m\omega_1$. Comme $a, \omega_1 \in \mathfrak{a}$ alors $-m\omega_1 \in \mathfrak{a}$ et $a - m\omega_1 \in \mathfrak{a}$ donc $\gamma \in \mathfrak{a}$. Par conséquent

$$\gamma = (\alpha_1 - m)\omega_1 + \alpha_2\omega_2 + \cdots + \alpha_n\omega_n,$$

et pour chaque injection $\sigma_i : K \to \mathbb{C}$ on a

$$\sigma_i(\gamma) = (\alpha_1 - m)\sigma_i(\omega_1) + \alpha_2\sigma_i(\omega_2) + \cdots + \alpha_n\sigma_i(\omega_n)$$

pour $1 \leq i \leq n$. Par la règle de Cramer

$$x_1 - m = \frac{\begin{vmatrix} \gamma & \alpha_2 & \dots & \alpha_n \\ \sigma_1(\gamma) & \sigma_1(\alpha_2) & \dots & \sigma_1(\alpha_n) \\ \vdots & \vdots & \dots & \vdots \\ \sigma_n(\gamma) & \sigma_n(\alpha_2) & \dots & \sigma_n(\alpha_n) \end{vmatrix}}{\begin{vmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \dots & \sigma_1(\alpha_n) \\ \vdots & \vdots & \dots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \dots & \sigma_n(\alpha_n) \end{vmatrix}}$$

donc $(x_1 - m)^2 = \frac{d(\gamma, \omega_2, \dots, \omega_n)}{d(\omega_1, \dots, \omega_n)}$. Par conséquent

$$0 < |d(\gamma, \omega_2, \dots, \omega_n)| = (\alpha_1 - m)^2 |d(\omega_1, \dots, \omega_n)| < |d(\omega_1, \dots, \omega_n)|$$

et $|d(\omega_1, \dots, \omega_n)|$ n'est pas l'élément minimal comme supposé. En conclusion, tous les éléments $\alpha_1, \dots, \alpha_n \in \mathbb{Z}$ et $\mathfrak{a}$ est un $\mathbb{Z}$-module libre de rang n. □

Rappelons qu'un anneau A est Noetherien si tout ensemble non vide d'idéaux de A possède un plus grand élément au sens de l'inclusion. De manière équivalente, A est un anneau est Noetherien si tout idéal est engendré par un nombre fini d'éléments. Une autre caractérisation est que toute suite de croissante d'idéaux de A est stationnaire. En d'autres termes, si

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \cdots \subseteq \mathfrak{a}_{n-1} \subseteq \mathfrak{a}_n \subseteq \dots$$

est une suite croissante d'idéaux de A, alors il existe un rang k à partir duquel $\mathfrak{a}_m = \mathfrak{a}_{m+1}$ pour tout $m \geq k$.

Théorème 5.17. *Soit $K/\mathbb{Q}$ une extension finie. Alors O_K est un anneau Noetherien.*

Démonstration. Par la proposition précédente tout idéal $\mathfrak{a}$ de O_K est un $\mathbb{Z}$-module de rang fini. Cela implique que $\mathfrak{a}$ est un O_K-module de type fini et que chaque idéal est donc engendré par un nombre fini d'éléments. Par le paragraphe précédent, O_K est donc un anneau Noetherien. □

5.4 Anneaux de Dedekind

Cette partie s'inspire plus particulièrement de [1]. Rappelons nous qu'un idéal $\mathfrak{a} \subseteq A$ est premier si $\mathfrak{a}|\mathfrak{bc} \implies \mathfrak{a}|\mathfrak{b}$ ou $\mathfrak{a}|\mathfrak{c}$ pour tout idéal $\mathfrak{b}, \mathfrak{c} \subseteq A$. Ce n'est pas sans rappeler la notion d'élément premier d'un anneau.

Définition 5.15. Un anneau de Dedekind est un anneau intègre Noetherien, intégralement clos et tel que tout idéal premier non nul est maximal.

Théorème 5.18. *Soit K un corps de nombres et O_K son anneau des entiers. Alors O_K est un anneau de Dedekind.*

Démonstration. Par la propriété 5.13, O_K est intègre. Par le théorème 5.15, O_K est intégralement clos et par le théorème 5.17, O_K est Noetherien. Reste à montrer que tout idéal premier non nul est maximal. Soit $\mathfrak{p}$ un idéal premier non nul de O_K. Alors $\mathfrak{p} \cap \mathbb{Z}$ est un idéal premier de $\mathbb{Z}$. En effet, soient $a, b \in \mathbb{Z}$. Si $ab \in \mathfrak{p} \cap \mathbb{Z}$ alors en particulier $ab \in \mathfrak{p}$ et comme $\mathfrak{p}$ est un idéal premier, $a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$. Cela montre que $a \in \mathfrak{p} \cap \mathbb{Z}$ ou $b \in \mathfrak{p} \cap \mathbb{Z}$ donc $\mathfrak{p} \cap \mathbb{Z}$ est une idéal premier de p. On vérifie que cet idéal n'est pas l'idéal nul. □

Lemme 5.19. *Soit A un anneau Noetherien et soit $\mathfrak{a} \subset A$ un idéal non nul de A. Alors il existe des idéaux premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \subset A$ tel que $\mathfrak{p}_1 \ldots \mathfrak{p}_n \subseteq \mathfrak{a}$.*

Démonstration. Supposons qu'il existe des idéaux non nuls ne vérifiant pas le lemme et soit $\mathcal{I}$ l'ensemble de ces idéaux. Comme A est Noetherien, toute suite d'idéaux croissante est stationnaire et il existe un idéal $\mathfrak{a}$ de $\mathcal{I}$ qui n'est contenu dans aucun autre idéal de $\mathcal{I}$. Comme $\mathfrak{a}$ ne peut pas contenir d'idéal premier il ne peut, en particulier, être lui-même un idéal premier. Par conséquent, il existe des éléments $x, y \in \mathfrak{a}$ avec $xy \in \mathfrak{a}$ mais tel que $x \notin \mathfrak{a}$ et $y \notin \mathfrak{a}$. De ce fait, les idéaux $\mathfrak{a}_1 = Ax + \mathfrak{a}$ et $\mathfrak{a}_2 = Ay + \mathfrak{a}$ contiennent chacun $\mathfrak{a}$ strictement et donc $\mathfrak{a}_1, \mathfrak{a}_2 \notin \mathcal{I}$. Dès lors, il existe des idéaux premiers non nuls $\mathfrak{p}_1, \ldots, \mathfrak{p}_j \subset A$ et $\mathfrak{p}_{j+1}, \ldots, \mathfrak{p}_n \subset A$ tel que $\mathfrak{p}_1 \ldots \mathfrak{p}_j \subseteq \mathfrak{a}_1$ et $\mathfrak{p}_{j+1} \ldots \mathfrak{p}_n \subseteq \mathfrak{a}_2$. Mais $\mathfrak{a}_1\mathfrak{a}_2 = (Ax + \mathfrak{a})(Ay + \mathfrak{a}) = Axy + Ay\mathfrak{a} + Ax\mathfrak{a} + \mathfrak{a}^2 \subseteq A\mathfrak{a} + Ay\mathfrak{a} + Ax\mathfrak{a} + \mathfrak{a}^2 \subseteq \mathfrak{a}$. Cela montre que

$$\mathfrak{p}_1 \ldots \mathfrak{p}_n \subseteq \mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a},$$

ce qui entraîne une contradiction. En conclusion $\mathcal{I}$ est vide et tout idéal non nul vérifie le lemme. □

Définition 5.16. Soit O_K un anneau de Dedekind et soit K son corps des fractions. Soit de plus $\mathfrak{a}$ un idéal non nul de O_K. On pose

$$\mathfrak{a}^{-1} = \{x \in K \mid x\mathfrak{a} \subseteq A\}.$$

Proposition 5.20. *Soit $\mathfrak{p}$ un idéal premier de O_K. Alors $\mathfrak{p}\mathfrak{p}^{-1} = O_K$.*

Démonstration. Pour la preuve on suit [23]. À priori, $O_K \subseteq \mathfrak{p}^{-1}$, par définition de $\mathfrak{p}^{-1}$. On montre d'abord que $\mathfrak{p}^{-1} \neq O_K$. Soit $a \in \mathfrak{p}$ un élément non nul. Considérons $\langle a \rangle = aO_K$ l'idéal engendré par a. Par le lemme précédent, il existe des idéaux premiers de O_K tels que $\mathfrak{p}_1 \ldots \mathfrak{p}_n \subseteq \langle a \rangle \subseteq \mathfrak{p}$. Supposons que n est

minimal pour cette propriété. Si $\mathfrak{p}_i \neq \mathfrak{p}$ pour tout $1 \leq i \leq n$, alors il existerait des éléments $x_i \in \mathfrak{p}_i$ avec $x_i \notin \mathfrak{p}$ de sorte que $x_1 \dots x_n \in \mathfrak{p}$ mais $x_1, \dots x_n, \notin \mathfrak{p}$. Ceci est impossible puisque $\mathfrak{p}$ est un idéal premier. Sans perte de généralité, supposons que $\mathfrak{p}_1 = \mathfrak{p}$. Par la minimalité de n, on sait que $\mathfrak{p}_2 \dots \mathfrak{p}_n \not\subseteq \langle a \rangle$. Il existe donc un $b \in \mathfrak{p}_2 \dots \mathfrak{p}_n$ tel que $b \notin \langle a \rangle = aO_K$. Dès lors $a^{-1}b \notin O_K$. Mais comme $\mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_n = \mathfrak{p}\mathfrak{p}_2 \dots \mathfrak{p}_n \subseteq \langle a \rangle$, on sait que $b\mathfrak{p} \subseteq \langle a \rangle = aO_K$. Cela montre que $a^{-1}b\mathfrak{p} \subseteq O_K$, c'est-à-dire, par définition de $\mathfrak{p}^{-1}$, que $a^{-1}b \in \mathfrak{p}^{-1}$. On a donc trouvé un élément qui est dans $\mathfrak{p}^{-1}$ mais qui n'est pas dans O_K. Donc $\mathfrak{p}^{-1} \neq O_K$. Reste à démontrer que $\mathfrak{p}\mathfrak{p}^{-1} \neq \mathfrak{p}$, car alors $\mathfrak{p} \subset \mathfrak{p}\mathfrak{p}^{-1}$ et comme $\mathfrak{p}$ est maximal, la seule possibilité est que $\mathfrak{p}\mathfrak{p}^{-1} = O_K$. Supposons que $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$ et soit $\omega_1, \dots, \omega_m$ une base pour $\mathfrak{p}$ (O_K est Noetherien). Alors pour tout $x \in \mathfrak{p}$ il existe des $a_{ij} \in O_K$ tel que $x\omega_i = a_{i1}\omega_1 + \dots + a_{im}\omega_m$ pour tout $1 \leq i \leq m$ de sorte que

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{2m-1} & a_{1m} \\ \vdots & \vdots & \dots & \vdots & \vdots \\ a_{i1} & \dots & a_{ii} - x & \dots & a_{im} \\ \vdots & \vdots & \dots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mm-1} & a_{mm} \end{pmatrix} \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_i \\ \vdots \\ \omega_m \end{pmatrix} = 0.$$

En notant A la matrice carré à gauche on a $\det(A) = 0$ car les $\omega_i \neq 0$. Mais $\det(A)$ est un polynôme à coefficients dans O_K et x est donc racine d'un polynôme de $O_K[X]$. Par conséquent $x \in O_K$ et $\mathfrak{p}^{-1} \subseteq O_K$ ce qui contredit ce que nous avons montré précédemment. Par conséquent $\mathfrak{p}\mathfrak{p}^{-1} \neq \mathfrak{p}$ et ceci achève la démonstration. □

Comme $O_K = \langle 1 \rangle$, on voit que $\mathfrak{p}\mathfrak{p}^{-1} = \langle 1 \rangle$ et on comprend que $\mathfrak{p}^{-1}$ joue le rôle de l'élément inverse de $\mathfrak{p}$. Cependant $\mathfrak{p}^{-1}$ n'est pas un idéal de O_K puisque $\mathfrak{p}^{-1} \not\subseteq O_K$.

Définition 5.17. Un idéal fractionnaire de O_K est un ensemble non vide $\mathfrak{a} \subset K$ tel que pour tout $a, b \in \mathfrak{a}$ et pour tout $c \in O_K$ on a $a + b \in \mathfrak{a}$, $ca \in \mathfrak{a}$ et il existe $d \in O_K$ non nul tel que $d\mathfrak{a} \subseteq O_K$.

En particulier tout idéal de O_K est un idéal fractionnaire. Avec cette définition on voit aussi que $\mathfrak{p}^{-1}$ est un idéal fractionnaire de O_K.

Théorème 5.21. *Soit A un anneau de Dedekind et soit $\mathfrak{a} \subset A$ un idéal non nul. Alors $\mathfrak{a}$ admet une factorisation en produit d'idéaux premiers non nuls*

$$\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_n,$$

unique à permutation des facteurs près.

Démonstration. On suit [23] (théorème 3.3). Supposons que l'ensemble $\mathcal{I}$ des idéaux qui n'admettent pas de factorisation en idéaux premiers non nuls est non vide. Comme A est Noetherien, on sait qu'il existe un idéal maximal $\mathfrak{a} \in \mathcal{I}$ au sens de l'inclusion. Par le lemme 5.19 il existe des idéaux premiers non nuls $\mathfrak{p}_1, \dots, \mathfrak{p}_n \subset A$ tel que $\mathfrak{p}_1 \dots \mathfrak{p}_n \subseteq \mathfrak{a}$. Supposons n minimal pour cette propriété.

Si $n = 1$ alors $\mathfrak{p}_1 \subseteq \mathfrak{a}$ et comme $\mathfrak{p}_1$ est maximal, $\mathfrak{a} = \mathfrak{p}_1$ ce qui contredit l'hypothèse que $\mathfrak{a} \in \mathcal{I}$. Supposons donc que $n \geq 2$. Par la proposition 5.20, $\mathfrak{p}_1^{-1}\mathfrak{p}_1 = A$ donc

$$\mathfrak{p}_1^{-1}\mathfrak{p}_1 \dots \mathfrak{p}_n = A\mathfrak{p}_2 \dots \mathfrak{p}_n = \mathfrak{p}_2 \dots \mathfrak{p}_n$$

et par conséquent

$$\mathfrak{p}_1^{-1}\mathfrak{a} \supseteq \mathfrak{p}_2 \dots \mathfrak{p}_n.$$

Comme $A \subset \mathfrak{p}_1$ on a $A\mathfrak{a} = \mathfrak{a} \subset \mathfrak{p}_1\mathfrak{a}$. Maintenant si $\mathfrak{a} = \mathfrak{p}^{-1}\mathfrak{a}$ alors $\mathfrak{p}_2 \dots \mathfrak{p}_n \subseteq \mathfrak{a}$ ce qui contredit la minimalité de n. Donc $\mathfrak{a} \subset \mathfrak{p}^{-1}\mathfrak{a}$. Comme $\mathfrak{p}^{-1}\mathfrak{a}$ est un idéal de A mais que $\mathfrak{p}^{-1}\mathfrak{a} \notin \mathcal{I}$, on en déduit qu'il existe des idéaux premiers non nuls $\mathfrak{q}_2, \dots, \mathfrak{q}_m$ tel que

$$\mathfrak{p}^{-1}\mathfrak{a} = \mathfrak{q}_2 \dots \mathfrak{q}_m.$$

Mais alors

$$\mathfrak{a} = \mathfrak{a}A = \mathfrak{a}\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}_1\mathfrak{q}_2 \dots \mathfrak{q}_m$$

et cela montre que $\mathfrak{a} \notin \mathcal{I}$ ce qui contredit l'hypothèse.

Il reste à montrer l'unicité. Soient

$$\mathfrak{p}_1 \dots, \mathfrak{p}_n = \mathfrak{q}_1 \dots \mathfrak{q}_m$$

deux factorisations différentes de $\mathfrak{a}$ en idéaux premiers non nuls. Comme $\mathfrak{q}_1 \dots \mathfrak{q}_m \subset \mathfrak{p}_1$ et que $\mathfrak{p}_1$ est un idéal premier alors il existe un $1 \leq i \leq m$ tel que $\mathfrak{q}_i \subseteq \mathfrak{p}_1$. Sans perte de généralité on peut supposer que $i = 1$. Mais alors $\mathfrak{p}_1 = \mathfrak{q}_1$ puisque $\mathfrak{q}_1$ est maximal. En multipliant des deux côtés de l'égalité par $\mathfrak{p}_1^{-1} = \mathfrak{q}_1^{-1}$, cela montre que

$$\mathfrak{p}_2 \dots \mathfrak{p}_n = \mathfrak{q}_2 \dots \mathfrak{q}_m.$$

Par récurrence cela montre que $n = m$ et $\mathfrak{p}_i = \mathfrak{q}_i$ pour tout $1 \leq i \leq n$. □

Si on regroupe les facteurs communs on peut évidemment écire

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_n^{e_n}.$$

Proposition 5.22. *L'ensemble des idéaux fractionnaires de O_K forme un groupe pour le produit.*

La preuve découle du théorème 5.21.

Proposition 5.23. *Si $\mathfrak{a}$ et $\mathfrak{b}$ sont des idéaux de O_K alors*

$$\mathfrak{a} \subseteq \mathfrak{b} \iff \mathfrak{b} \text{ divise } \mathfrak{a}.$$

Démonstration. On a $\mathfrak{a} \subseteq \mathfrak{b} \iff \mathfrak{a}\mathfrak{b}^{-1} \subseteq \mathfrak{b}\mathfrak{b}^{-1}$. Mais alors $\mathfrak{a}\mathfrak{b}^{-1} \subseteq O_K$, c'est-à-dire que $\mathfrak{a}\mathfrak{b}^{-1}$ est un idéal de O_K. Soit $\mathfrak{c}$ cet idéal. Dès lors $\mathfrak{c} = \mathfrak{a}\mathfrak{b}^{-1}$, ou encore $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ et $\mathfrak{b}$ divise $\mathfrak{a}$. □

Chez les idéaux il suffit donc de retenir que "contenir c'est diviser". Avec cette proposition on se rend bien compte que les idéaux maximaux ne peuvent pas être divisés. Les idéaux maximaux jouent donc le rôle de des éléments irréductibles dans O_K. Dans un anneau de Dedekind, ces deux notions coïncident de la même manière que les éléments irréductibles et les éléments premiers d'un anneau factoriel coïncident.

5.5 Théorie de ramification de Hilbert

On s'inspire du chapitre 1 section 9 de [23]. Soit $\mathfrak{p}$ un idéal premier (non nul) d'un corps de nombres K. Soit L/K une extension galoisienne finie. Notons O_L et O_K l'anneau des entiers de L et K respectivement. Par ce que nous avons vu précédemment, tout idéal de L possède une unique factorisation en idéaux premiers. Par la proposition 5.23, les seuls idéaux de L qui divisent $\mathfrak{p}$ vu comme un idéal de L sont les idéaux $\mathfrak{P} \subseteq L$ qui contiennent $\mathfrak{p}$. Soit

$$\mathfrak{p}L = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g}$$

cette factorisation unique. On appelle e_i **l'indice de ramification** de $\mathfrak{p}$ en $\mathfrak{P}_i$. On sait que $O_L/\mathfrak{P}_i$ est un corps (on peut montrer que c'est **fini**) car $\mathfrak{P}_i$ est maximal (c'est un idéal premier dans un anneau de Dedekind). Le degré

$$[O_L/\mathfrak{P}_i : O_K/\mathfrak{p}] = f_i,$$

est appelé **le degré d'inertie** de $\mathfrak{p}$ en $\mathfrak{P}_i$. Si on note $n = [L : K]$, alors on peut montrer qu'on a la relation [12]

$$n = \sum_{i=1}^{g} e_i f_i.$$

Cette formule se simplifie grandement lorsque l'on prend en compte le fait que L/K est une extension galoisienne. Soit $\sigma \in \mathrm{Gal}(L/K)$. Comme $\mathfrak{p}O_K$ est maximal et que $\mathfrak{p} \subseteq \mathfrak{P}_i$, on a $\mathfrak{p} \cap O_K = \mathfrak{P}_i \cap O_K$. Donc $\sigma(\mathfrak{p} \cap O_K) = \mathfrak{p} \cap O_K = \sigma(\mathfrak{P}_i \cap O_K) = \sigma(\mathfrak{P}_i) \cap O_K$ et $\sigma(\mathfrak{P}_i)$ est un autre idéal premier de O_L contenant $\mathfrak{p}$ ($\sigma(O_L) = O_L$ car les conjugués des éléments de O_L sont aussi des éléments qui sont racines d'un polynôme monique à coefficients dans O_K). Dans ce cas, il se trouve que $\mathrm{Gal}(L/K)$ agit transitivement sur les idéaux $\mathfrak{P}_i$. Cela signifie que pour tout $1 \leq i, j \leq g$, il existe $\sigma \in \mathrm{Gal}(L/K)$ de sorte que $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$. En appliquant σ à la formule de la factorisation de $\mathfrak{p}$ on a

$$\sigma(\mathfrak{p}) = \mathfrak{p} = \sigma(\mathfrak{P}_1)^{e_1} \dots \sigma(\mathfrak{P}_g)^{e_g} = \mathfrak{P}_1^{k_1} \dots \mathfrak{P}_1^{k_g} = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g}.$$

Donc $k_i = e_i$ pour tout $1 \leq i \leq g$ et on en déduit que tous les $e_i := e$ sont en fait égaux. On montre aussi que tous les degrés d'inerties sont égaux. La relation des degrés se simplifie dans le cas galoisien en

$$n = efg,$$

où g est le nombre de facteurs de $\mathfrak{p}$ dans L, e l'indice de ramification commun et f le degré d'inertie commun des $\mathfrak{P}_i$. Ces indices dépendent de l'idéal premier $\mathfrak{p}$ et pour bien faire il faudrait ajouter les indices $e := e_\mathfrak{p}, f := f_\mathfrak{p}, g := g_\mathfrak{p}$. Pour résumer, $\mathfrak{p} = (\mathfrak{P}_1 \dots \mathfrak{P}_g)^e$ dans L. Soit maintenant E/L une extension galoisienne finie de K (donc une extension galoisienne finie de L). Dans cette

12. Cette relation fonctionne pour n'importe quelle extension L/K séparable. Dans le cas galoisien, il y a mieux.

extension, les $\mathfrak{P}_i$ possèdent eux-même une factorisation en idéaux premiers dans E. On a donc $\mathfrak{P}_1 = (\mathfrak{q}_1 \dots \mathfrak{q}_{g'})^{e'}$ où $e' = e_{E/L}$ est l'indice de ramification de $\mathfrak{P}_1$ dans E etc... de sorte qu'en injectant cette factorisation dans la factorisation de $\mathfrak{p}$ dans L on a

$$\mathfrak{p} = ((\mathfrak{q}_1 \dots \mathfrak{q}_{g'})^{e'} \dots)^e$$

dans E. Par conséquent $e_{E/K} = e_{E/L}e_{L/K}$, $g_{E/K} = g_{E/L}g_{L/K}$ et par le théorème 3.23 on a aussi $f_{E/K} = f_{E/L}f_{L/K}$.

Définition 5.18. Le groupe de décomposition en $\mathfrak{P}$ sur K est

$$G_{\mathfrak{P}} = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

Le corps fixé par ce groupe est $Z_{\mathfrak{P}} = \mathrm{Fix}(G_{\mathfrak{P}})$. Toujours en posant $[L : K] = n = efg$, on a la proposition suivante.

Proposition 5.24. *Soit $\mathfrak{P}$ un idéal premier de L. Soit $\mathfrak{q} = \mathfrak{P} \cap Z_{\mathfrak{P}}$ un idéal de $Z_{\mathfrak{P}}$. Alors $[Z_{\mathfrak{P}} : K] = g$ et $[L : Z_{\mathfrak{P}}] = ef$.*

Démonstration. Par le théorème fondamental de la théorie de Galois $\mathrm{Gal}(L/Z_{\mathfrak{P}}) = G_{\mathfrak{P}}$. Par conséquent, l'indice de $G_{\mathfrak{P}}$ dans $\mathrm{Gal}(L/K)$ est g. Donc $[Z_{\mathfrak{P}} : K] = g$. □

Cela montre aussi que $\mathfrak{q}$ possède un indice de ramification et un degré d'inertie égal à 1 sur K. De même, $\mathfrak{P}$ possède un indice de ramification égal à e sur $Z_{\mathfrak{P}}$ et un degré d'inertie égal à f. Par conséquent, $\mathfrak{q}O_L = \mathfrak{P}^e$ et il n'y a pas d'autres idéaux qui interviennent dans la décomposition de $\mathfrak{q}$ dans O_L. On a donc la suite de corps $K \subseteq Z_{\mathfrak{P}} \subseteq L$ et la suite de corps résiduels $\kappa(\mathfrak{p}) = \kappa(\mathfrak{q}) \subseteq \kappa(\mathfrak{P})$. Si on se concentre sur la partie $L/Z_{\mathfrak{P}}$, on voit qu'un élément de $G_{\mathfrak{P}}$ induit un automorphisme naturel $\overline{\sigma} : \kappa(\mathfrak{P}) \to \kappa(\mathfrak{P}) : x \bmod \mathfrak{P} \mapsto \sigma(x) \bmod \mathfrak{P}$ qui est en fait un élément de $\mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$.

Proposition 5.25. *L'homomorphisme*

$$G_{\mathfrak{P}} \to Gal(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$$

est surjectif.

Démonstration. On s'inspire de [23] (prop. 9.4 chapitre 1) qui contient une démonstration plus générale.

Comme $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ est une extension galoisienne finie, nous savons par le théorème de l'élément primitif qu'il existe un $\overline{\alpha} \in \kappa(\mathfrak{P})$ tel que $\kappa(\mathfrak{P}) = \kappa(\mathfrak{p})(\overline{\alpha})$. Soit $\overline{m}_{\overline{\alpha}}(X)$ son polynôme minimal sur $\kappa(\mathfrak{p})$. Un élément $\overline{\sigma} \in \mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$ envoie $\overline{\alpha}$ sur une autre racine de $\overline{m}_{\alpha}(X)$. On a donc $\overline{\sigma}(\overline{\alpha}) = \overline{\beta}$ avec $\overline{m}_{\overline{\alpha}}(\overline{\beta}) = 0$. Soit α un élément de O_L tel que $\alpha \equiv \overline{\alpha} \bmod \mathfrak{P}$. Notons $m_\alpha(X)$ son polynôme minimal sur K. Comme $m_\alpha(\alpha) = 0$ on a $m_\alpha(\overline{\alpha}) \equiv 0 \bmod \mathfrak{P}$. Par conséquent toutes les racines de $\overline{m}_{\overline{\alpha}}(X)$ sont aussi des racines de $m_\alpha(X) \bmod \mathfrak{P}$. Il existe donc un élément $\beta \in O_L$ tel que $\beta \equiv \overline{\beta} \bmod \mathfrak{P}$ avec $m_\alpha(\beta) = 0$. Maintenant si β est une racine de $m_\alpha(X)$ alors il existe $\sigma \in G_{\mathfrak{P}}$ tel que $\sigma(\alpha) = \beta$. Mais alors

$$\overline{\beta} \equiv \sigma(\alpha) \equiv \overline{\sigma}(\overline{\alpha}) \bmod \mathfrak{P},$$

et donc l'homomorphisme est surjectif. □

En notant $I_{\mathfrak{P}}$ le noyau de cette surjection on a

$$G_{\mathfrak{P}}/I_{\mathfrak{P}} \cong \mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})).$$

Ce noyau est, par définition, l'ensemble des $\sigma \in G_{\mathfrak{P}}$ tels que $\sigma(x) \equiv x \bmod \mathfrak{P}$.

Définition 5.19. Le sous-groupe $I_{\mathfrak{P}} \subseteq G_{\mathfrak{P}}$ est appelé le groupe d'inertie de L/K. Le corps $T_{\mathfrak{P}} = \mathrm{Fix}(I_{\mathfrak{P}})$ est appelé le corps inertiel.

Par le théorème fondamental de la théorie de Galois, $G_{\mathfrak{P}}/I_{\mathfrak{P}} \cong \mathrm{Gal}(T_{\mathfrak{P}}/Z_{\mathfrak{P}})$ et, par définition, $\mathrm{Gal}(L/T_{\mathfrak{P}}) = I_{\mathfrak{P}}$. Maintenant, le groupe d'inertie de L/K est le même que celui de $L/T_{\mathfrak{P}}$. Par la proposition 5.25, on a donc $\mathrm{Gal}(L/T_{\mathfrak{P}})/I_{\mathfrak{P}} \cong 1 \cong \mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{q}_T))$ où $\mathfrak{q}_T = \mathfrak{P} \cap O_{T_{\mathfrak{P}}}$. Mais alors $\kappa(\mathfrak{q}_T) = \kappa(\mathfrak{P})$ et $[L : T_{\mathfrak{P}}] = e$. Par la multiplicativité des degrés on a aussi $[T_{\mathfrak{P}} : Z_{\mathfrak{P}}] = f$.

Le diagramme suivant est sans doute, avec la factorisation en idéaux premiers dans les anneaux de Dedekind, le résultat le plus important de ce chapitre. Il résume les quelques résultats précédents et illustre comment un idéal premier de K se factorise au fil des extensions associées aux sous-groupes clefs de $\mathrm{Gal}(L/K)$.

$$\begin{array}{ccccc}
L & \longleftarrow & \langle 1 \rangle & \longrightarrow & \mathfrak{p} = (\mathfrak{P}_1 \dots \mathfrak{P}_g)^e \\
\mathrm{e}\,\big| & & \big| & & \\
T_{\mathfrak{P}} & \longleftarrow & I_{\mathfrak{P}} & \longrightarrow & \mathfrak{p} = \mathfrak{P}_1 \dots \mathfrak{P}_g \\
\mathrm{f}\,\big| & & \big| & & \\
Z_{\mathfrak{P}} & \longleftarrow & G_{\mathfrak{P}} & \longrightarrow & \mathfrak{p} = \mathfrak{P}_1 \dots \mathfrak{P}_g \\
\mathrm{g}\,\big| & & \big| & & \\
K & \longleftarrow & G & \longrightarrow & \mathfrak{p}
\end{array}$$

Example 5.26. Soit $a \in \mathbb{Q}$ un nombre qui n'est pas un carré. Considérons l'extension $K = \mathbb{Q}(\sqrt{a})$. Soit $p > 2$ un nombre premier (le cas $p = 2$ agit un peu différemment). On souhaite savoir de quelle façon p se factorise dans $\mathbb{Q}(\sqrt{a})$. Comme $[\mathbb{Q}(\sqrt{a}) : \mathbb{Q}] = 2 = efg$, nous savons qu'il n'y a que trois possibilités :

1. p est totalement décomposé : $e = 1$, $f = 1$, $g = 2$ donc $pO_K = \mathfrak{p}_1\mathfrak{p}_2$.
2. p est totalement ramifié : $e = 2$, $f = 1$, $g = 2$ donc $pO_K = \mathfrak{p}^2$.
3. p est inerte : $e = 1$,$f = 2$,$g = 1$ donc pO_K est encore un idéal premier.

On peut montrer que ces trois cas dépendent de la nature de a mod p. Précisément, le cas 1) survient lorsque a est un carré modulo p, le cas 2) lorsque a est un multiple de p et le cas 3) lorsque a n'est pas un carré modulo p. Prenons par exemple $a = 3$. Alors $K = \mathbb{Q}(\sqrt{3})$ et on peut montrer que $O_K = \mathbb{Q}[\sqrt{3}]$.

Considérons le nombre premier 5. On a $3 \not\equiv x^2 \bmod 5$ pour tout $x \in \mathbb{Z}/5\mathbb{Z}$ car les carrés de $\mathbb{Z}/5\mathbb{Z}$ sont $0, 1, 4$. Par conséquent, 5 est encore un nombre premier dans O_K. De manière équivalente, $5O_K$ est un idéal premier de O_K, ou encore 5

est inerte. Pour voir cela, supposons qu'il existe une factorisation de 5 dans O_K. Dans ce cas, il existe deux éléments irréductibles $\alpha = c + d\sqrt{3}$ et $\beta = e + f\sqrt{3}$ dans O_K tels que $5 = (c + d\sqrt{3})(e + f\sqrt{3})$. Mais alors $5^2 = (c^2 - 3d^2)(e^2 - 3f^2)$ et on a $\pm 5 = (c^2 - 3d^2)$ ou $\pm 5 = (e^2 - 3f^2)$. Mais l'équation $5 = x^2 - 3y^2$ ne possède pas de solution dans $\mathbb{Z}$. En effet

$$5 \equiv 2 \equiv x^2 - 3y^2 \equiv x^2 \bmod 3$$

et 2 n'est pas un carré dans $\mathbb{Z}/3\mathbb{Z}$. L'équation $-5 = x^2 - 3y^2$ ne possède pas non plus de solution car

$$-5 \equiv 3 \equiv x^2 - 3y^2 \equiv x^2 + y^2 \bmod 4,$$

ce qui est impossible car les carrés de $\mathbb{Z}/4\mathbb{Z}$ sont 0 et 1. Cela montre que 5 est bien irréductible dans O_K.

Considérons ensuite le nombre premier 11. On a $3 \equiv 5^2 \bmod 11$, donc 3 est un carré dans $\mathbb{Z}/11\mathbb{Z}$. Il existe donc deux idéaux premiers distincts $\mathfrak{p}_1, \mathfrak{p}_2 \subset O_K$ tel que $11O_K = \mathfrak{p}_1\mathfrak{p}_2$. On montre que les idéaux

$$\mathfrak{p}_1 = \langle 11, 5 + \sqrt{3} \rangle = \{11k_1 + (5 + \sqrt{3})k_2 \mid k_1, k_2 \in \mathbb{Z}\}$$

et

$$\mathfrak{p}_1 = \langle 11, 5 - \sqrt{3} \rangle = \{11k_1 + (5 - \sqrt{3})k_2 \mid k_1, k_2 \in \mathbb{Z}\}$$

conviennent. En premier lieu, on vérifie facilement que ces idéaux sont premiers en montrant qu'ils sont maximaux (nous ne le faisons pas). Ensuite, il s'agit de montrer que $\mathfrak{p}_1 \neq \mathfrak{p}_2$. On a $5 - \sqrt{3} \in \mathfrak{p}_2$ mais $5 - \sqrt{3} \notin \mathfrak{p}_1$ car sinon il existerait $k_1, k_2 \in \mathbb{Z}$ tels que

$$5 - \sqrt{3} = 11k_1 + (5 + \sqrt{3})k_2.$$

L'égalité montre que $k_2 = -1$, donc on a $5 = 11k_1 - 5$ ce qui est impossible, par conséquent $\mathfrak{p}_1 \neq \mathfrak{p}_2$. Enfin on a que $\mathfrak{p}_1\mathfrak{p}_2 = 11O_K$. En effet,

$$\begin{aligned}
\mathfrak{p}_1\mathfrak{p}_2 &= \{11^2k_1 + 11(5 - \sqrt{3})k_2 + 11(5 + \sqrt{3})k_3 - 22k_4 \mid k_1, k_2, k_3, k_4 \in \mathbb{Z}\} \\
&= \langle 11^2, 11(5 - \sqrt{3}), 11(5 + \sqrt{3}), -22 \rangle \\
&= \langle 11 \rangle \langle 11, 5 - \sqrt{3}, 5 + \sqrt{3}, -2 \rangle.
\end{aligned}$$

Mais les nombres $2, -11, (5 - \sqrt{3} + 5 + \sqrt{3})$ sont dans $\langle 11, 5 - \sqrt{3}, 5 + \sqrt{3}, -2 \rangle$. Par conséquent $2 - 11 + (5 - \sqrt{3} + 5 + \sqrt{3}) = 1 \in \langle 11, 5 - \sqrt{3}, 5 + \sqrt{3}, -2 \rangle$ et donc cet idéal est l'anneau O_K tout entier. Dès lors $\mathfrak{p}_1\mathfrak{p}_2 = 11O_K$.

Reste à illustrer le cas d'un nombre premier qui se ramifie totalement. Le seul cas possible est $p = 3$, car c'est le seul nombre premier qui divise 3. On montre que l'idéal $\mathfrak{p} = \langle 3, \sqrt{3} \rangle$ vérifie $3O_K = \langle 3 \rangle = \mathfrak{p}^2$. À nouveau il est facile de voir que $\mathfrak{p}$ est maximal et donc premier. De plus,

$$\begin{aligned}
\mathfrak{p}^2 &= \langle 3, \sqrt{3} \rangle \langle 3, \sqrt{3} \rangle \\
&= \langle 9, 3\sqrt{3}, 3 \rangle \\
&= \langle 3 \rangle \langle 3, \sqrt{3}, 1 \rangle
\end{aligned}$$

et clairement $1 \in \langle 3, \sqrt{3}, 1 \rangle$ donc $\langle 3, \sqrt{3}, 1 \rangle = O_K$ de sorte que $\langle 3 \rangle = \mathfrak{p}^2$.

5.6 Application aux extensions cyclotomiques

Entre la théorie et la pratique il reste beaucoup de chemins. Nous énonçons les résultats suivants sans les démontrer.

Proposition 5.27. *Soit ζ_n une racine primitive n-ième de l'unité. L'anneau des entiers de l'extension cyclotomique $\mathbb{Q}(\zeta_n)$ est $\mathbb{Z}[\zeta_n]$.*

Théorème 5.28. *Soit p un nombre premier et soit $n = p^r m$ où $pgcd(p, m) = 1$. Soit ζ_n une racine primitive n-ième de l'unité et soit $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ l'extension cyclotomique associée. Alors*

$$p\mathbb{Z}[\zeta_n] = (\mathfrak{p}_1 \dots \mathfrak{p}_g)^{\varphi(p^r)},$$

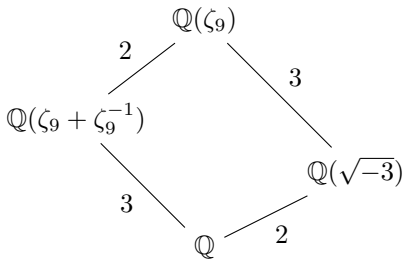
où le degré d'inertie f commun à tous les $\mathfrak{p}_i$ est le plus petit entier tel que $p^f \equiv 1 \ mod\ m$.

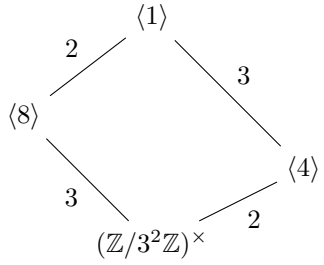
En d'autres termes, l'indice de ramification est $e = \varphi(p^r)$, f divise $\varphi(m)$ et, par la relation $\varphi(n) = efg$, on a $g = \frac{\varphi(n)}{\varphi(p^r)f}$.

Reprenons l'exemple du chapitre 2 tronqué à $\mathbb{Q}(\zeta_9)/\mathbb{Q}$. Nous savons que $\mathrm{Gal}(\mathbb{Q}(\zeta_9)/\mathbb{Q}) \cong (\mathbb{Z}/9\mathbb{Z})^\times$ et $[\mathbb{Q}(\zeta_9) : \mathbb{Q}] = \varphi(9) = 6$. Les sous-groupes non triviaux de $(\mathbb{Z}/9\mathbb{Z})^\times$ sont $\langle 8 \bmod 9\rangle$ d'ordre 2 et $\langle 4 \bmod 9\rangle = \langle 7 \bmod 9\rangle$ d'ordre 3. Le corps fixé par $\langle 4 \bmod 9\rangle$ est $\mathbb{Q}(\zeta_3) = \mathbb{Q}\big(\frac{1}{2} + i\frac{\sqrt{3}}{2}\big) = \mathbb{Q}(\sqrt{-3})$. Pour trouver le corps fixé par $\langle 8 \bmod 9\rangle$, considérons un automorphisme $\sigma \neq \mathrm{id}$ représentant un élément de $\langle 8 \bmod 9\rangle$ et notons que l'élément

$$\alpha = \mathrm{id}(\zeta_9) + \sigma(\zeta_9) = \zeta_9 + \zeta_9^8 = \zeta_9 + \zeta_9^{-1} = 2\cos\big(\frac{2\pi}{9}\big) \in \mathbb{Q}(\zeta_9)$$

est invariant par l'action de σ, car $\sigma(\alpha) = \sigma(\mathrm{id}(\zeta_9)) + \sigma^2(\zeta_9) = \sigma(\zeta_9) + \mathrm{id}(\zeta_9) = \alpha$. Maintenant, avec un peu de trigonométrie, $(2\cos\big(\frac{2\pi}{9}\big))^3 = 6\cos\big(\frac{2\pi}{9}\big) - 1$ et on a la relation $\alpha^3 = 3\alpha - 1$. Dès lors, α est racine du polynôme $X^3 - 3X + 1 \in \mathbb{Q}[X]$. Les racines de ce polynôme sont $2\cos\big(\frac{2k\pi}{9}\big)$ pour $k = 1, 2, 4$. Ce polynôme est donc irréductible sur $\mathbb{Q}$ et $\mathbb{Q}(\alpha) = \mathbb{Q}(\zeta_9 + \zeta_9^{-1}) = \mathbb{Q}\big(2\cos\big(\frac{2\pi}{9}\big)\big)$ est l'extension fixée par $\langle 8 \bmod 9\rangle$. On a $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Pour résumer,





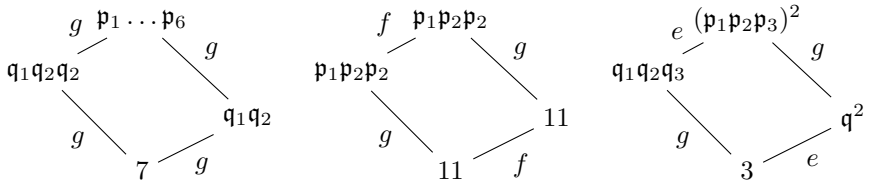
Par le théorème 5.28 nous savons que si un nombre premier p ne divise pas le degré de l'extension $\mathbb{Q}(\zeta_9)/\mathbb{Q}$ alors l'indice de ramification $e = 1$. Dans ce

cas, on a la relation $6 = efg = fg$. Prenons par exemple $p = 7$ et calculons son degré d'inertie. Il est clair que $7^1 \equiv 1 \bmod 6$. Par conséquent $f = 1$ et $g = 6$. Autrement dit 7 est complètement décomposé dans $\mathbb{Z}[\zeta_9]$ et il existe 6 idéaux premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_6$ distincts tel que $7\mathbb{Z}[\zeta_9] = \mathfrak{p}_1 \ldots \mathfrak{p}_6$. Cela signifie que $\mathbb{Q}(\zeta_9)$ est égal au corps de décomposition associé, c'est-à-dire, en utilisant les notations précédentes $\mathbb{Q}(\zeta_9) = Z_7$ et $\mathrm{Gal}(\mathbb{Q}(\zeta_9)/\mathbb{Q}) = G_7$. Considérons maintenant le cas $p = 11$. À nouveau p ne divise pas 6, donc $e = 1$. Cependant, contrairement à 7, on a $11^1 \not\equiv 1 \bmod 6$ mais $11^2 \equiv 1 \bmod 6$, donc $f = 2$. On a alors $g = 3$ et il existe 3 idéaux premiers $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ (différents des idéaux de la factorisation de 7) distincts tels que $11\mathbb{Z}[\zeta_9] = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$. Notons que par le théorème d'Euler (d'arithmétique modulaire), il n'est pas possible que $f > 2 = \varphi(6)$, donc aucun nombre premier $p > 3$ est inerte ($f = 6$, $g = 1$, $e = 1$ est impossible). Considérons ensuite $p = 2$. On a $6 = 2^1 3$. Dès lors, l'indice de ramification est donné par $e = \varphi(2) = 1$. Le degré d'inertie vérifie $2^f \equiv 1 \bmod 3$, donc $f = 2$. Par la relation $6 = efg = 2g$ on trouve $g = 3$. Par le même raisonnement que précédemment il y a trois idéaux premiers distincts de $\mathbb{Z}[\zeta_9]$ tels que $2\mathbb{Z}[\zeta_9] = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$. Finalement prenons $p = 3$. On a $e = \varphi(3) = 2$. Ensuite $3^1 \equiv 1 \bmod 2$ donc $f = 1$. En combinant les résultats on a $g = 3$ et il y a trois idéaux de $\mathbb{Z}[\zeta_9]$ tels que $3\mathbb{Z}[\zeta_9] = (\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3)^2$.

Regardons maintenant la factorisation des nombres $7, 11, 3$ dans $\mathbb{Q}(\sqrt{-3})$. Par l'exemple 5.26 (ou par le fait que $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3)$ et appliquant le théorème 5.28) nous savons que $p > 2$ se factorise en un produit de deux idéaux premiers si et seulement si -3 est un carré modulo p. Ensuite $p > 2$ reste inerte si et seulement si -3 n'est pas un carré modulo p et finalement p est totalement ramifié si et seulement si p divise -3. Pour $p = 7$ nous avons que $-3 \equiv 4 \bmod 7$ est un carré. Donc il existe des idéaux premiers distincts $\mathfrak{q}_1, \mathfrak{q}_2$ tels que $7O_{\mathbb{Q}(\sqrt{-3})} = \mathfrak{q}_1\mathfrak{q}_2$. Au vu de la factorisation de 7 dans $\mathbb{Z}[\zeta_9]$ nous savons comment $\mathfrak{q}_1$ et $\mathfrak{q}_2$ se décomposent dans $\mathbb{Z}[\zeta_9]$. À une permutation des indices près, $\mathfrak{q}_1 = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ tandis que $\mathfrak{q}_2 = \mathfrak{p}_4\mathfrak{p}_5\mathfrak{p}_6$. Maintenant reprenons $p = 11$. On a $-3 \equiv 8 \bmod 11$. Mais 8 n'est pas un carré dans $\mathbb{Z}/11\mathbb{Z}$. Par conséquent 11 est inerte et $11O_{\mathbb{Q}(\sqrt{-3})}$ est un idéal premier. Par les calculs précédents, nous savons que $11O_{\mathbb{Q}(\sqrt{-3})}$ se factorise dans $\mathbb{Z}[\zeta_9]$ comme $\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$. Prenons encore $p = 3$. On a $3|-3$, donc 3 est totalement ramifié et il existe un idéal premier $\mathfrak{q}$ de $O_{\mathbb{Q}(\sqrt{-3})}$ tel que $3O_{\mathbb{Q}(\sqrt{-3})} = \mathfrak{q}^2$. Au vu de la factorisation de 3 dans $\mathbb{Z}[\zeta_9]$ on sait que $\mathfrak{q} = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_2$ dans $\mathbb{Z}[\zeta_9]$.

En fait nous aurions pu déduire la factorisation des éléments des nombres premiers dans $O_{\mathbb{Q}(\sqrt{-3})}$ à partir de la factorisation de ces derniers dans $\mathbb{Z}[\zeta_9]$ car si on a une tour d'extension $K \subset E \subset L$ avec $e_{L/K}, f_{L/K}, g_{L/K}$ et $e_{E/K}, f_{E/K}, g_{E/K}$ et $e_{L/E}, f_{L/E}, g_{L/E}$ les indices de ramifications, d'inerties et de décompositions respectifs, alors $e_{L/K} = e_{E/K}e_{L/E}$, $f_{L/K} = f_{E/K}f_{L/E}$, $g_{L/K} = g_{E/K}g_{L/E}$. En appliquant ce résultat à l'extension $\mathbb{Q}(\zeta_9 + \zeta_9^{-1})/\mathbb{Q}$ on en déduit tout de suite les factorisations suivantes. Pour $p = 7$ alors $7O_{\mathbb{Q}(\zeta_9+\zeta_9^{-1})} = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$ pour des idéaux premiers distincts $\mathfrak{q}_1, \mathfrak{q}_2\mathfrak{q}_3$ de $O_{\mathbb{Q}(\zeta_9+\zeta_9^{-1})}$. À une permutation des indices près, on a $\mathfrak{q}_1 = \mathfrak{p}_1\mathfrak{p}_2$, $\mathfrak{q}_2 = \mathfrak{p}_3\mathfrak{p}_4$, $\mathfrak{q}_3 = \mathfrak{p}_5\mathfrak{p}_6$. Pour $p = 11$ on a $11O_{\mathbb{Q}(\zeta_9+\zeta_9^{-1})} = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$. En comparant les factorisations de 11 dans $O_{\mathbb{Q}(\zeta_9+\zeta_9^{-1})}$ et celle de $\mathbb{Z}[\zeta_9]$ on a

(à une permutation près) $\mathfrak{q}_1 = \mathfrak{p}_1$, $\mathfrak{q}_2 = \mathfrak{p}_2$, $\mathfrak{q}_3 = \mathfrak{p}_3$. Pour $p = 3$, il reste $3O_{\mathbb{Q}(\zeta_9+\zeta_9^{-1})} = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$ où les $\mathfrak{q}_i$ sont chaque fois distincts pour chaque nombre premier. On sait que $\mathfrak{q}_1 = \mathfrak{p}_1^2$, $\mathfrak{q}_2 = \mathfrak{p}_2^2$, $\mathfrak{q}_3 = \mathfrak{p}_3^2$ dans $\mathbb{Z}[\zeta_9]$. On peut résumer les étapes de la factorisation avec les diagrammes suivants.



Nous avons indiqué par la lettre e, f ou g l'unique changement d'une extension à l'autre.

6 Théorie de Galois différentielle

Le chapitre se base sur les oeuvres [6],[11],[13],[19],[25],[34].

6.1 Introduction

Le sujet du chapitre n'est plus l'étude des équations polynomiales par les corps et les groupes. Ici les équations différentielles linéaires joueront le rôle analogue des polynômes de la théorie précédente, les corps différentiels remplaceront les corps, et les groupes seront munis d'une topologie. Il existe une correspondance galoisienne pour les corps différentiels ainsi qu'une condition nécessaire et suffisante de résolubilité d'une équation différentielle linéaire par des fonctions élémentaires. Tous les anneaux considérés dans cette section sont unitaires et commutatifs.

Commençons par deux exemples qui vont motiver ce chapitre.

Soit l'équation différentielle

$$y''(x) = \frac{y(x)}{x^2}, \tag{5}$$

avec des conditions initiales non fixées. Cette équation est un cas particulier de l'équation différentielle d'Euler

$$x^2y''(x) + axy'(x) + by(x) = 0$$

pour $a = 0$ et $b = -1$. En cherchant une solution de la forme x^α on a

$$(x^\alpha)'' = x^\alpha/x^2,$$

ou encore

$$\alpha(\alpha-1)x^{\alpha-2} = x^{\alpha-2},$$

de sorte que α doit vérifier l'équation $\alpha^2 - \alpha - 1 = 0$. Les deux racines de ce polynôme sont $\alpha_1 = \frac{1+\sqrt{5}}{2}$ et $\alpha_2 = \frac{1-\sqrt{5}}{2}$ donc x^{α_1} et x^{α_2} sont des solutions de l'équation 5. Comme ces deux solutions sont linéairement indépendantes et que l'ensemble des solutions d'une EDO du second degré forme un espace vectoriel de dimension 2 sur $\mathbb{C}$ on sait que l'ensemble des solutions de l'équation 5 est

$$E = \{k_1 x^{\alpha_1} + k_2 x^{\alpha_2} \mid k_1, k_2 \in \mathbb{C}\}$$

où k_1 et k_2 dépendent du choix des conditions initiales $y(0)$ et $y'(0)$.

Considérons maintenant l'équation différentielle

$$y''(x) = xy(x), \tag{6}$$

en apparence plus simple que l'équation précédente. À nouveau les conditions initiales ne sont pas fixées. Supposons que les solutions peuvent s'écrire sous la forme $y(x) = \sum_{n=0}^{+\infty} a_n x^n$, alors

$$\left(\sum_{n=0}^{+\infty} a_n x^n\right)'' = x\left(\sum_{n=0}^{+\infty} a_n x^n\right)$$

c'est-à-dire,

$$\sum_{n=0}^{+\infty}(n+2)(n+1)a_{n+2}x^n = \sum_{n=0}^{+\infty} a_n x^{n+1}.$$

En identifiant les termes de même monôme on trouve $a_2 = 0$ et

$$(n+3)(n+2)a_{n+3} = a_n$$

pour tout $n \geq 0$. Les premières itérations donnent $a_0 = 3.2a_3$, $a_1 = 4.3a_4$, $a_2 = 5.4a_5 = 0$, $a_3 = 6.5a_6$, $a_4 = 7.6a_7$, $a_5 = 8.7a_8 = 0$, $a_6 = 9.8a_9$ etc... Les valeurs de a_0 et a_1 dépendent des conditions initiales. Ainsi les solutions de l'équation 6 peuvent toutes s'écrire sous la forme

$$y(x) = a_0\left(\sum_{n=0}^{+\infty} \frac{x^{3n}}{(2.3)(5.6)\dots(3n-1)(3n)}\right) + a_1\left(\sum_{n=0}^{+\infty} \frac{x^{3n+1}}{(3.4)(6.7)\dots(3n)(3n+1)}\right).$$

Lorsque l'on pose $a_0 = \frac{1}{3^{2/3}\Gamma(\frac{2}{3})}$ et $a_1 = \frac{-1}{3^{1/3}\Gamma(\frac{1}{3})}$ (où Γ est la fonction Gamma d'Euler) la solution $Ai(x) := y(x)$ est aussi connue sous le nom de fonction d'Airy. Pour les conditions initiales $a_0 = \frac{1}{3^{1/6}\Gamma(\frac{2}{3})}$ et $a_1 = \frac{3^{1/6}}{\Gamma(\frac{1}{3})}$ la solution $Bi(x) := y(x)$ est appelée la fonction Bi d'Airy. Ensemble, $Ai(x)$ et $Bi(x)$ forment un système fondamental de solutions (comme les séries présentes dans l'expression de $y(x)$) pour l'équation 6, donc l'ensemble des solutions de cette équation est

$$E = \{k_1 Ai(x) + k_2 Bi(x) \mid k_1, k_2 \in \mathbb{C}\}.$$

Les fonctions d'Airy ne sont pas des fonctions dites élémentaires. De la même manière que pour les polynômes en théorie de Galois classique, nous voudrions savoir si une équation différentielle est résoluble par des combinaisons de fonctions élémentaires (comme la première) ou non (comme pour la seconde). Pour cela il nous faut définir ce que l'on entend par "combinaisons" et par "fonctions élémentaires". Il nous faudra aussi développer la théorie de Galois des équations différentielles car la résolubilité d'une équation différentielle dépendra de la résolubilité de son groupe de Galois différentiel. Cette théorie comporte de nombreux parallèles avec la théorie de Galois classique et nous ne serons pas en mesure d'expliciter toutes les preuves. Pour combler ce manque nous tenterons de faire le plus de liens possibles avec les autres chapitres et présenterons davantage d'exemples.

6.2 Anneaux et corps différentiels

Il est possible de faire de la théorie de Galois différentielle en caractéristique p mais cela nous emmènerait trop loin. Tous les corps de ce chapitre sont supposés de caractéristique 0.

Définition 6.1. Un anneau différentiel est un anneau A muni d'une dérivation $\partial : A \to A$ vérifiant les propriétés

$$\partial(x+y) = \partial(x) + \partial(y)$$

et

$$\partial(xy) = \partial(x)y + x\partial(y)$$

pour tout $x, y \in A$.

Si A est un corps, on parle de corps différentiel. On note parfois (A, ∂) pour préciser la dérivation associée à l'anneau A.

Example 6.1. L'exemple générique est le corps $\mathbb{C}(t)$ des fonctions rationnelles à coefficients dans $\mathbb{C}$, de variable t muni de la dérivation usuelle $\frac{d}{dt}$ est un corps différentiel. Pour notre exposé, ce corps différentiel va jouer le même rôle que $\mathbb{Q}$ en théorie de Galois classique.

Définition 6.2. L'ensemble des constantes C_A d'un anneau différentiel A est défini comme

$$C_A = \{\partial(x) = 0 \mid x \in A\}.$$

Notons que $0 \in C_A$ et $1 \in C_A$ car

$$\partial(0) = \partial(0+0) = \partial(0) + \partial(0)$$

donc $\partial(0) = 0$ et

$$\partial(1) = \partial(1.1) = 1.\partial(1) + \partial(1).1$$

donc $\partial(1) = 0$. Vu les propriétés de la dérivation, si $x, y \in C_A$ alors $x + y \in C_A$ et $xy \in C_A$. On a

Proposition 6.2. *Si A est un anneau (corps) différentiel, alors C_A est un anneau (corps).*

Démonstration. Si A est un anneau différentiel le résultat est direct. Si A est un corps différentiel alors il s'agit de montrer que tout élément non nul dans C_A possède un inverse. Pour cela, il faut déterminer la dérivation d'un quotient. Soient $x \in A$ quelconque et $y \in A$ non nul,

$$\partial(x) = \partial\left(\frac{xy}{y}\right) = \partial(y)\frac{x}{y} + y\partial\left(\frac{x}{y}\right)$$

donc

$$\partial\left(\frac{x}{y}\right) = \frac{\partial(x)y - x\partial(y)}{y^2}.$$

En choisissant $x = 1 \in C_A$ et $y \in C_A$ non nul on a

$$\partial(y^{-1}) = -\frac{\partial(y)}{y^2} = 0,$$

d'où $y^{-1} \in C_A$. □

On montre par récurrence que la dérivation ∂ vérifie les propriétés usuelles de la dérivation classique,

— $\partial(x^n) = nx^{n-1}\partial(x)$

— $\partial^n(xy) = \sum_{i=0}^{n} C_n^i \partial^i(x)\partial^{n-i}(y)$

pour tout $n \geq 1$.

6.3 Extensions de dérivation

Définition 6.3. Un idéal I d'un anneau différentiel (A, ∂) est un idéal différentiel de A si $a \in I$ implique que $\partial(a) \in I$.

Définition 6.4. Un homomorphisme différentiel d'anneaux différentiels $\varphi : (A, \partial_A) \to (B, \partial_B)$ est un homomorphisme d'anneaux vérifiant $\varphi(\partial_A(x)) = \partial_B(\varphi(x))$ pour tout $x \in A$.

Proposition 6.3. *Le noyau d'un homomorphisme différentiel $\varphi : (A, \partial_A) \to (B, \partial_B)$ est un idéal différentiel de A.*

Démonstration. Clairement $\mathrm{Ker}(\varphi)$ est un idéal de A. De plus, si $\varphi(x) = 0$ alors $\varphi(\partial_A(x)) = \partial_B(\varphi(x)) = \partial_B(0) = 0$. Donc $\mathrm{Ker}(\varphi)$ est un idéal stable pour la dérivation, c'est-à-dire un idéal différentiel de A. □

La construction n'est pas triviale, mais on peut montrer que la dérivation d'un corps différentiel K se prolonge de manière unique à n'importe quelle extension algébrique L/K. Voir [6] (théorème 6.2.6). Si $L = K(X)$ et si l'extension L/K est transcendante alors il existe une dérivation ∂_L sur L qui prolonge celle de K et qui est telle que $\partial_L(X) = a$ pour n'importe quel choix de $a \in L$. Voir [34] (Exercice 3 ch. 1). Ces deux résultats montrent que dans tous les cas, les extensions des corps différentiels sont encore des corps différentiels cohérents pour la dérivation sur K.

6.4 Equations différentielles

Soit (K, ∂) un corps différentiel. Considérons l'équation différentielle

$$\partial^n y + k_{n-1}\partial^{n-1} y + \dots k_1 \partial y + k_0 Y = 0,$$

avec $k_0, \dots, k_{n-1} \in K$. Il est connu que cette équation différentielle homogène peut se réécrire sous la forme matricielle

$$\partial Y = AY,$$

en posant $Y = (y_1, \dots, y_n)$, $\partial Y = (\partial y_1, \dots, \partial y_n)$ et

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & \dots & \dots & 1 \\ -k_0 & -k_1 & -k_2 & \dots & \dots & -k_{n-1} \end{pmatrix} \in K^{n\times n}.$$

L'ensemble des solutions de cette équation matricielle forme un espace vectoriel de dimension n sur le corps des constantes C_K de K. En particulier l'ensemble des solutions qui sont dans K^n forme un espace vectoriel de dimension au plus n. En général les solutions ne sont pas dans K^n, de la même manière qu'en général, un polynôme ne possède pas ses racines dans le corps de ses coefficients.

Définition 6.5. Une matrice fondamentale pour le système $\partial Y = AY$ est une matrice inversible $B \in K^{n\times n}$ telle que $\partial B = AB$.

Définition 6.6. Soit (K, ∂) un corps différentiel et soit $\partial Y = AY$ avec $A \in K^{n\times n}$. Supposons qu'il existe une matrice fondamentale $B = (b)_{ij} \in K^{n\times n}$ pour le système. L'extension L/K est dite de Picard-Vessiot si

— L est le plus petit corps différentiel qui contient K et les b_{ij}

— $C_L = C_K$.

Une extension de Picard-Vessiot joue le même rôle que le corps de décomposition dans la théorie de Galois classique. Comme pour ce dernier, on peut montrer que pour tout système $\partial Y = AY$, cette extension **existe** et est **unique** (à isomorphisme près).

6.5 Groupe de Galois différentiel

Définition 6.7. Soit (L, ∂_L) une extension du corps différentiel (K, ∂_K). Le groupe de Galois différentiel de cette extension est défini comme l'ensemble des automorphismes de L qui fixent K et qui commutent avec la dérivation sur L. On le note

$$\mathrm{Gal}_\partial(L/K) = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma \circ \partial_L = \partial_L \circ \sigma\}.$$

Soit $A \in \mathbb{K}^{n\times n}$ et soit

$$\partial Y = AY,$$

une équation différentielle sous sa forme matricielle. Soit L l'extension de Picard-Vessiot de cette équation.

Proposition 6.4. *Si B est une matrice fondamental de l'équation $\partial Y = AY$ alors pour tout $\sigma \in Gal_{\partial_L}(L/K)$ la matrice $\sigma(B) = C$ est aussi une solution du système.*

Démonstration. Par définition $\partial B = AB$. En appliquant $\sigma \in \mathrm{Gal}_{\partial_L}(L/K)$ à cette équation on a $\sigma(\partial(B)) = \sigma(AB) = \sigma(A)\sigma(B)$. Comme les entrées de A sont dans K on a $\sigma(A)$ et comme σ commute avec la dérivation de L, $\sigma(\partial(B)) = \partial(\sigma(B))$. Au final il reste $\partial(\sigma(B)) = A\sigma(B)$ et $\sigma(B)$ est une nouvelle solution du système. □

Cette proposition est tout à fait analogue à la proposition 3.40 de la théorie de Galois classique. Ici les éléments du groupe de Galois différentiel se voient plutôt comme des matrices tandis que les éléments du groupe de Galois en théorie de Galois classique sont plutôt des vus comme des permutations (des racines des polynômes).

Example 6.5. Considérons l'équation $y' = ay$ avec $a \in \mathbb{C}$. Notons L son extension de Picard-Vessiot. Comme vu dans l'exemple X, une solution à cette équation est donnée par $y = e^{at} \in L$. Si $\sigma \in \mathrm{Gal}(L/K)$ alors par la proposition précédente, il existe un $k \in \mathbb{C}$ non nul [13] tel que $\sigma(e^{at}) = ke^{at}$. En outre σ est entièrement déterminé par son action sur e^{at} et on voit bien que que σ ne dépend que de la constante k. Par conséquent $\mathrm{Gal}_\partial(L/K) = \mathbb{C}^\times$.

Comme en théorie de Galois infinie, la structure algébrique des groupes n'est pas suffisante et il faut ajouter une structure topologique à $\mathrm{Gal}_\partial(L/K)$ pour obtenir une correspondance exacte. En théorie de Galois infinie, la topologie était celle de Krull. Ici la topologie est celle de **Zariski**. Les extensions de Picard-Vessiot vont aussi (un peu comme le corps de décomposition d'un polynôme séparable est une extension galoisienne) jouer le rôle des extensions galoisiennes en ce sens que c'est avec ce type d'extension que l'on obtient une correspondance galoisienne entre corps différentiels intermédiaires de l'extension L/K et les sous-groupes fermés de $\mathrm{Gal}_\partial(L/K)$ pour la topologie de Zariski.

Théorème 6.6. *(Théorème fondamental de la théoire de Galois différentielle) Soit K un corps différentiel. Soit $\partial Y = AY$ un équation différentielle avec $A \in K^{n\times n}$. Notons L/K l'extension de Picard-Vessiot de l'équation différentielle. Alors il y a une correspondance entre l'ensemble des sous-groupes fermés pour la topologie de Zariski de $Gal_\partial(L/K)$ et l'ensemble des corps différentiels intermédiaires de L/K.*

Démonstration. La preuve peut être trouvée dans [34] (théorème 1.27). □

13. sinon σ ne serait pas un automorphisme

6.6 Extensions de Liouville

Les extensions de Liouville jouent le rôle analogue des extensions radicales de la théorie de Galois classique. Soit L/K une extension de corps différentiels. Si $\alpha \in L$ est tel que $\alpha' = a \in K$, alors α est appelé une intégrale de a. Si $b' = \alpha'/\alpha \in K$ alors on dit que α est une exponentielle (de l'intégrale) de b.

Définition 6.8. L'extension L/K est dite de Liouville s'il existe une tour d'extension

$$K = K_1 \subseteq K_2 \subseteq \cdots \subseteq K_{n-1} \subseteq K_n = L,$$

où pour tout $1 \leq i \leq n-1$, $K_{i+1} = K_i(\alpha_i)$ où α_i est soit
— une intégrale d'un élément de K_i
— une exponentielle d'un élément de K_i
— un élément algébrique sur K_i.

Notons quand même qu'une exponentielle ou une intégrale d'un élément de K ne peut pas être algébrique sur K. Si on suppose par exemple que $\alpha \in L$ est une intégrale sur K alors il existe $a \in K$ tel que $\alpha' = a$ et il existe un polynôme monique de degré minimal $m_\alpha^K(X) = \sum_{i=0}^n k_i X^i \in K[X]$ tel que $m_\alpha^K(\alpha) = 0$. En dérivant cette relation on trouve

$$n\alpha^{n-1}a + k'_{n-1}\alpha^{n-1} + k_{n-1}(n-1)a\alpha^{n-2} + k'_{n-2}\alpha^{n-2} + \cdots + ak_1 + k'_0 = 0,$$

qui est un polynôme de degré $n-1$ s'annulant en α. Donc ses coefficients doivent être nuls et en particulier $na + k'_{n-1} = 0$. C'est impossible puisque car $a = \alpha'$.

Théorème 6.7. *Soit K un corps différentiel et soit l'équation $Y' = AY$, avec $A \in K^{n\times n}$. Notons L l'extension de Picard-Vessiot de l'équation en question. Alors L est contenue dans une extension de Liouville si et seulement si la composante connexe de l'identité G_0 de $Gal_\partial(L/K)$ est résoluble.*

Démonstration. La preuve est dans [25] (ch.6). □

Être contenu dans une extension de Liouville est synonyme d'être résoluble par des fonctions élémentaires.

Proposition 6.8. *Le groupe $SL(2,\mathbb{C})$ est connexe et n'est pas résoluble.*

Démonstration. La preuve est dans l'article [11]. □

En particulier, cela montre que la composante connexe de l'identité de $\mathrm{SL}(2,\mathbb{C})$ est le groupe tout entier. Pour voir que l'équation différentielle $y'' = xy$ n'est pas résoluble par des fonctions élémentaires, il faut montrer que son groupe de Galois différentiel n'est pas résoluble. En fait, on montre (voir [13]) que son groupe est justement $\mathrm{SL}(2,\mathbb{C})$ lorsque l'on regarde l'équation différentielle sur le corps différentiel $\mathbb{C}(x)$ muni de la dérivée usuelle. Ce genre de méthodes permettent aussi de montrer que certaines fonctions ne sont pas élémentaires en les regardant comme des solutions d'équations différentielles (linéaires).

7 Théorie de Galois des revêtements

Le chapitre se base sur les ouvrages [9],[14],[15],[27].

7.1 Introduction

Il y a une similarité remarquable entre la théorie de Galois classique et la théorie des revêtements. Informellement, partant d'un espace topologique connecté (par exemple le plan $\mathbb{C}$, un graphe connecté, un cercle, un tore, une sphère etc...) on définit un groupe, appelé groupe fondamental, qui est l'ensemble des courbes fermées que l'on peut tracer sur cette surface modulo les déformations continues (aussi présent dans théorie des noeuds). Ce groupe est un invariant topologique, c'est-à-dire que deux espace topologiques homéomorphes possèdent le même groupe fondamental. Inversement, deux espaces topologiques qui possèdent un groupe fondamental différent ne sont pas homéomorphes. À un espace topologique X, on associe des revêtements, qui sont des espaces topologiques muni d'une projection sur X. Ces revêtements ressemblent localement à X mais sont plus "grands" que X. Comme un revêtement est encore un espace topologique, il possède lui aussi un groupe fondamental. Il se trouve que ce groupe fondamental est isomorphe à un sous-groupe du groupe fondamental de l'espace topologique X. De la même manière que dans la théorie de Galois classique, il existe une correspondance entre l'ensemble des sous-groupes du groupe fondamental de X et l'ensemble des revêtements connectés de X. Le revêtement associé au sous-groupe trivial $\langle 1 \rangle$ est appelé le revêtement universel de X. Cette théorie est liée à la théorie de Galois différentielle et à la théorie de Galois classique par les dessins d'enfants de Grothendieck (Il y a un lien entre le groupe de Galois absolu de $\mathbb{Q}$ et le "complété profini" du groupe fondamental de la sphère privée de trois points. (Voir théorie de Grothendieck-Teichmüller.)).

7.2 Préliminaires

Lemme 7.1. *(Lemme de recollement) Soient X et Y des espaces topologiques. Soit $A = \cup_{i \in I} A_i \subset X$ un ensemble qui peut s'écrire comme une union finie de fermés $A_i \subset X$. Soient $f_i : A_i \to Y$ des fonctions continues pour tout $i \in I$. Supposons que $f_i(A_i \cap A_j) = f_j(A_i \cap A_j)$ pour tout $i, j \in I$. Alors il existe une unique fonction continue $F : A \to Y$ tel que $F|_{A_i} = f_i$ pour tout $i \in I$.*

Démonstration. Pour tout $i \in I$ on pose $F(a) = f_i(a)$ si $a \in A_i$. Cette fonction est la seule qui soit telle que $F|_{A_i} = f_i$ pour tout $i \in I$. Il reste à montrer la continuité. Soit C un fermé de Y. Soit $a \in A$. Alors $F(a) \in C$ si et seulement il existe f_i tel que $f_i(a) \in C$. Par conséquent $F^{-1}(C) = \cup f_i^{-1}(C)$. Comme f_i est continue pour chaque i, $f_i^{-1}(C)$ est fermé dans A_i. Mais une union finie de fermés est encore un fermé et $F^{-1}(C)$ est fermé dans A. Cela montre que l'image réciproque de tout fermé de Y est un fermé de A, donc F est une fonction continue. □

7.3 Chemins et groupe fondamental

On se donne un espace topologique X. Sur cet espace on va considérer des "chemins". Un chemin sur X est une fonction continue $\gamma : I = [0,1] \to X$. Intuitivement, si X est une surface "gentille" on peut s'imaginer un chemin comme le résultat d'un trait de crayon continu sur celle-ci. Un chemin possède un point initial $x_0 = \gamma(0)$ et un point final $x_f = \gamma(1)$. Si le point initial et le point final du chemin γ coïncident on dit que γ est un lacet. Si de plus $\gamma(t) = \gamma(0)$ pour tout $t \in [0,1]$ alors γ est appelé un lacet **constant**. Si tout couple de point $(x,y) \in X \times X$ peut être joint par un chemin, c'est-à-dire s'il existe un chemin γ sur X tel que $\gamma(0) = x$ et $\gamma(1) = y$, alors on dit que X est connexe par arcs.

Soient γ_1, γ_2 deux chemins sur X. Supposons que ces chemins soient tels que $\gamma_1(1) = \gamma_2(0)$. La **composition** de deux chemins $\gamma = \gamma_1.\gamma_2$ peut être définie de la façon suivante

$$\gamma(t) = \begin{cases} \gamma_1(2t) & \text{si } 0 \leq t \leq \frac{1}{2} \\ \gamma_2(2t-1) & \text{si } 1/2 \leq t \leq 1. \end{cases}$$

On vérifie que γ est bien un chemin. Il est défini sur $[0,1]$ et à valeur dans X. Sa continuité est induite par le fait que γ_1 et γ_2 sont des fonctions continues sur le fermé $[0,1]$ et que $\gamma_1(1) = \gamma_2(0)$. Il est évident que si γ_3 est un chemin tel que $\gamma_2(1) = \gamma_3(0)$ alors

$$(\gamma_1.\gamma_2).\gamma_3 = \gamma_1.(\gamma_2.\gamma_3).$$

Autrement dit, la composition est une loi **associative**. Supposons maintenant que $\gamma_2(t) = \gamma_1(1-t)$ (c'est encore un chemin). Il suit que $\gamma_1(1) = \gamma_2(0)$ et la composition $z = \gamma_1.\gamma_2$ est un chemin qui parcourt d'abord γ_1 puis γ_2. En fait $z : [0,1] \to X$ a pour point initial $\gamma_1(0)$ et pour point final $\gamma_1(0)$, c'est donc un lacet. Il faut cependant faire attention que z n'est pas un lacet constant.

Notons L_x l'ensemble des lacets sur X dont l'extrémité est x. La loi de composition des chemins restreinte à cet ensemble est alors une loi de composition interne. De plus, la composition est associative. L'élément neutre est le lacet, c'est-à-dire le lacet qui ne bouge pas du point x. Cependant, cet ensemble ne forme pas un groupe car il est impossible de composer deux lacets pour obtenir l'élément neutre. Supposons que γ_1 et γ_2 soient deux lacets de L_x. Il semble légitime de penser que si $\gamma_2(t) = \gamma_1(1-t)$ alors γ_2 constitue un bon candidat pour définir le symétrique de γ_1.

Définition 7.1. Soit X un espace topologique. Soient deux chemins $\gamma_1, \gamma_2 : [0,1] \to X$ tel que $u = \gamma_1(0) = \gamma_2(0)$ et $v = \gamma_1(1) = \gamma_2(1)$. Les chemins γ_1 et γ_2 sont dits homotopes s'il existe une fonction continue $f : [0,1] \times [0,1] \to X$ tel que $f(0,t) = \gamma_1(t)$, $f(1,t) = \gamma_2(t)$ et $f(s,0) = u$, $f(s,1) = v$. Dans ce cas, on note $\gamma_1 \sim \gamma_2$ et la fonction f est appelée une homotopie des chemins γ_1 et γ_2.

En clair, la fonction[14] f déforme continûmenent γ_1 sans changer les extrémités u et v pour obtenir γ_2. Pour $0 < s < 1$ fixé et $t \in [0,1]$, $f(s,t)$ correspond

14. en fait c'est plutôt la famille des fonctions définie par f qui contient toutes les déformations continues possibles des courbes γ_1 et γ_2

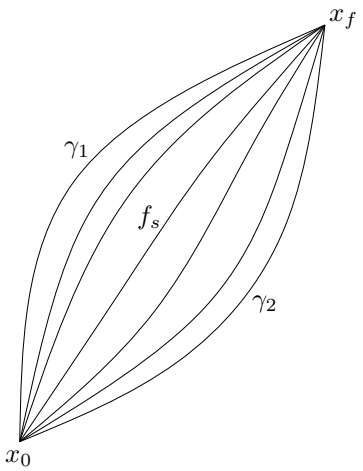


FIGURE 4 – Homotopie $\gamma_1 \sim \gamma_2$ avec $\gamma_1(0) = \gamma_2(0) = x_0$, $\gamma_1(1) = \gamma_2(1) = x_f$ et f_s représente un chemin intermédiaire $f(s,t)$ pour $0 < s < 1$ fixé. De plus, $f(0,t) = \gamma_1(t)$, $f(1,t) = \gamma_2(t)$.

à un chemin de point initial u et de point final v qui peut aussi être vu comme le résultat d'une déformation continue de γ_1 (Voir FIGURE 4).

Proposition 7.2. *La relation d'homotopie $\sim$ est une relation d'équivalence.*

Démonstration. Soit X un espace topologique. Soient $\gamma_1, \gamma_2, \gamma_3$ trois chemins définis sur X partageant les mêmes points extrémaux.

1) La relation est réflexive. L'homotopie $f(s,t) = \gamma_1(t)$ pour tout s montre que $\gamma_1 \sim \gamma_1$.

2) La relation est symétrique. Si $\gamma_1 \sim \gamma_2$ alors il existe une homotopie $f : [0,1] \times [0,1] \to X$ tel que $f(0,t) = \gamma_1(t)$ et $f(1,t) = \gamma_2(t)$. On voit alors que l'homotopie $g(s,t) := f(1-s,t)$ vérifie $g(0,t) = \gamma_2(t)$ et $g(1,t) = \gamma_1(t)$ donc $\gamma_2 \sim \gamma_1$.

3) La relation est transitive. Si $\gamma_1 \sim \gamma_2$ et $\gamma_2 \sim \gamma_3$ alors il existe deux homotopies f_1 et f_2 avec $f_1(0,t) = \gamma_1(t)$, $f_2(1,t) = \gamma_2(t)$ et $f_2(0,t) = \gamma_2(t)$, $f_2(1,t) = \gamma_3(t)$. On ne peut pas définir une nouvelle homotopie $f : [0,2] \times [0,1] \to X$ tel que $f(0,t) = \gamma_1(t)$ et $f(1,t) = \gamma_2(t)$ à cause du domaine $[0,2] \neq [0,1]$. Cependant

$$f(s,t) = \begin{cases} f_1(2s,t) & \text{si } 0 \leq s < \frac{1}{2} \\ f_2(2s-1,t) & \text{si } 1/2 \leq s \leq 1 \end{cases}$$

convient. La continuité de f provient de la continuité de f_1 et f_2 et du fait que $f_1(1,t) = f_2(0,t)$. Donc $\gamma_1 \sim \gamma_3$. □

On note $[\gamma]$ la classe d'équivalence du chemin γ.

Proposition 7.3. *Soit X un espace toplogique et soit $x \in X$. L'ensemble $\pi_1(X,x) := L_x/\sim = \{[\gamma] \mid \gamma \in L_x\}$ est un groupe pour la loi de composition $[\gamma_1][\gamma_2] = [\gamma_1.\gamma_2]$.*

Démonstration. Il est clair que la loi de composition est interne.

1) Soient $\gamma_1, \gamma_2, \gamma_3 \in L_x$. On a vu que $\gamma_1.(\gamma_2.\gamma_3) = (\gamma_1.\gamma_2).\gamma_3$ donc $[\gamma_1][\gamma_2.\gamma_3] = [\gamma_1.\gamma_2][\gamma_3]$ et la loi de composition est associative.

2) L'élément neutre est la classe [id] des lacets homotopes au lacet constant. En effet, soit $\gamma \in L_x$, alors $\mathrm{id}.\gamma \sim \gamma$ via l'homotopie

$$f(s,t) = \begin{cases} \mathrm{id}(t) & \text{si } 0 \leq t < \frac{s}{2} \\ \gamma\left(\frac{2t-s}{2-s}\right) & \text{si } \frac{s}{2} \leq t \leq 1 \end{cases}$$

car $f(0,t) = \mathrm{id}(t)$ et $f(1,t) = \gamma(t)$. (le re-paramétrage de γ dans l'expression de $f(s,t)$ est aussi nécessaire pour que γ et id soit défini sur $[0,1]$.) La preuve de $\gamma.\mathrm{id} \sim \gamma$ est similaire et cela montre que [id] est l'élément neutre de $\pi_1(X,x)$.

3) L'élément $[\gamma]$ admet un inverse dans $\pi_1(X,x)$. Soit $\gamma^*(t) = \gamma(1-t)$. On montre que $[\gamma][\gamma^*] = [\mathrm{id}]$. Il s'agit de montrer que $\gamma.\gamma^* \sim \mathrm{id}$. L'homotopie qui convient est

$$f(s,t) = \begin{cases} \gamma(2t) & \text{si } 0 \leq t < \frac{s}{2} \\ \gamma(s) & \text{si } \frac{s}{2} \leq t \leq 1 - \frac{s}{2} \\ \gamma(2-2t) & \text{si } 1 - \frac{s}{2} \leq t \leq 1 \end{cases}$$

et on vérifie bien que $f(0,t) = \mathrm{id}(t)$ et $f(1,t) = \gamma(t).\gamma^*(t)$. □

7.4 Les revêtements

Définition 7.2. Soient X et Y deux espaces topologiques. Une application $f : X \to Y$ est un homéomorphisme si f est une bijection et si f^{-1} est continue.

Définition 7.3. Soit X un espace topologique. Un revêtement [15] de X est une espace topologique Y muni d'une surjection continue $p : Y \to X$ vérifiant les propriétés suivantes

1. pour tout $x \in X$ il existe un ouvert $U \subset X$ contenant x tel que $p^{-1}(U) = \cup_{i \in I} V_i$ où $V_i \subset Y$ est un ouvert $\forall i \in I$ et $V_i \cap V_j = \emptyset$ pour tout $i \neq j$.
2. $p|_{V_i} : V_i \to U$ est un homéomorphisme pour tout $i \in I$.

On note parfois (Y,p) le revêtement de X.

Définition 7.4. Soient X et Y deux espaces topologiques. Soit $p : \tilde{X} \to X$ un revêtement de X et soit l'application $f : Y \to X$. Un relèvement (*lift* en anglais) de f est une application $\tilde{f} : Y \to \tilde{X}$ tel que $p \circ \tilde{f} = f$.

Le lemme suivant est un résultat clef.

Lemme 7.4. *Soit $p : \tilde{X} \to X$ un revêtement. Soient de plus,*
- *$f : Y \times [0,1] \to X$ une fonction continue,*
- *$F_0 : Y \times \{0\} \to \tilde{X}$ une fonction continue qui relève $f|_{Y \times \{0\}} : Y \times \{0\} \to X$.*

Alors il existe un unique relèvement $F : Y \times [0,1] \to X$ de f tel que $F|_{Y \times \{0\}} = F_0$.

15. En général on dit plutôt que c'est la fonction p qui est le revêtement.

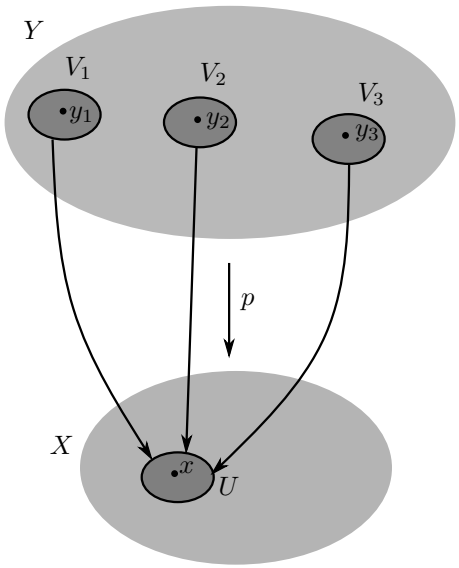


FIGURE 5 – Exemple de revêtement. Les images réciproques de x ($p^{-1}(x)$) sont y_1, y_2 et y_3. Chaque $p|_{V_i}(V_i)$ est homéomorphe à U.

Le diagramme suivant représente la situation.

$$\begin{array}{ccc} Y \times \{0\} & \xrightarrow{F_0} & \tilde{X} \\ {\scriptstyle i}\downarrow & \nearrow_{F} & \downarrow{\scriptstyle p} \\ Y \times [0,1] & \xrightarrow{f} & X \end{array}$$

La fonction $i : Y \times \{0\} \to Y \times [0,1]$ est l'injection canonique.

Démonstration. La preuve se fait en plusieurs étapes. On se base sur [9].

Soit $y \in Y$. Montrons d'abord qu'il est possible de trouver un voisinage V de y tel que $F : V \times [0,1] \to \tilde{X}$ est un relèvement de $f|_{V\times[0,1]}$ vérifiant $F_0 = F$ sur $V \times \{0\}$.

Par hypothèse, f est continue et il est donc possible de trouver un voisinage $V_t \times]a_t, b_t[$ de $(y,t) \in Y \times [0,1]$ tel que $f(V_t \times]a_t, b_t[) \subset U_t$ où U_t est un ouvert admissible de X contenant $f(y,t)$. Maintenant $\{y\} \times [0,1]$ est un sous-ensemble compact de $Y \times [0,1]$. Par conséquent il existe un nombre fini de sous-ensembles de $Y \times [0,1]$ qui recouvrent $y \times [0,1]$. En particulier, on peut choisir un ouvert $V \ni y$ ainsi qu'une subdivision $0 = t_0 < t_1 < \cdots < t_n = 1$ tel que $f(V \times [t_i, t_{i+1}])$ est contenu dans un ouvert admissible $U_i \subset X$. De cette façon, on a bien $\cup_i V \times [t_i, t_{i+1}] = V \times [0,1]$.

Par récurrence, supposons que le relèvement F du lemme est construit sur $V \times [0, t_i]$. Comme $f(V \times [t_i, t_{i+1}]) \subset U_i$ il existe $\tilde{U}_i \subset \tilde{X}$ contenant $F(y, t_i)$ tel

que $p|_{\tilde{U}_i} : \tilde{U}_i \to U_i$ est un homéomorphisme. En remplaçant V par un voisinage suffisamment petit de y on peut supposer que $F(V \times \{t_i\}) \subset \tilde{U}_i$. Maintenant, F doit vérifier $pF = f$. Or $p|_{\tilde{U}_i}$ est en bijection avec U_i, on peut donc considérer $p^{-1}|_{U_i}$. Dès lors, on peut définir F sur $V \times [t_i, t_{i+1}]$ comme étant la composition $F = p^{-1}|_{U_i} \circ f$. Maintenant $F_{V\times[0,t_i]}$ et $F_{V\times[t_i,t_{i+1}]}$ sont des fonctions continues qui coïncident en $V \times \{t_i\}$. Par le lemme des recollements, cela montre que $F|_{V\times[0,t_{i+1}]}$ est une fonction continue telle que $pF = f$ sur son domaine et $F_{V\times\{0\}} = F_0$. Par récurrence, cela montre que $F : V \times [0,1] \to \tilde{X}$ est un relèvement de f qui vérifie les hypothèses du lemme sur $V \times [0,1]$.

On montre maintenant que le relèvement F est unique lorsque Y est un singleton $\{y\}$. Le cas général sera déduit de cette démonstration. Soient F et G deux relèvements de $f : \{y\} \times [0,1]$ tel que $F(\{y\} \times \{0\}) = G(\{y\} \times \{0\})$. Par récurrence, supposons que $F = G$ sur $\{y\} \times [0, t_i]$. Comme $F(\{y\} \times [t_i, t_{i+1}])$ et $G(\{y\} \times [t_i, t_{i+1}])$ sont connectés dans $\tilde{X}$ et que $F(\{y\} \times [0, t_i]) = G(\{y\} \times [0, t_i])$ par hypothèse de récurrence, on en déduit que $F(\{y\} \times [t_i, t_{i+1}])$ et $G(\{y\} \times [t_i, t_{i+1}])$ appartiennent au même $\tilde{U}_i \subset \tilde{X}$. Comme $pF = pG$ sur $\tilde{U}_i$ et que p est un homéomorphisme, $F = G$ sur tout $\{y\} \times [t_i, t_{i+1}]$. Par récurrence, cela montre que $F = G$ sur tout $\{y\} \times [0,1]$. □

Proposition 7.5. *(Relèvement des chemins) Soit X un espace topologique.*
- *Soit $p : \tilde{X} \to X$ un revêtement.*
- *Soit $\gamma : [0,1] \to X$ un chemin avec comme point initial $x = \gamma(0)$.*
- *Soit $\tilde{x} \in p^{-1}(x)$ un élément dans la fibre de x.*

Alors il existe un unique relèvement $\tilde{\gamma} : [0,1] \to \tilde{X}$ du chemin γ avec pour point initial $\tilde{\gamma}(0) = \tilde{x}$.

Démonstration. Il suffit d'appliquer le lemme 7.4 avec Y un singleton quelconque $\{y\}$, f le chemin γ et $F_0(\{y\} \times \{0\}) = \tilde{x}$. Le relèvement F du lemme correspond au chemin $\tilde{\gamma}$. □

Proposition 7.6. *(Relèvement des homotopies) Soit X un espace topologique.*
- *Soit $p : \tilde{X} \to X$ un revêtement.*
- *Soit $f : [0,1] \times [0,1] \to X$ une homotopie de chemins partant de $x \in X$*
- *Soit $\tilde{x} \in p^{-1}(x)$ un élément dans la fibre de x.*

Alors il existe un unique relèvement d'homotopies de chemins partant de $\tilde{x}$.

Démonstration. On applique le lemme précédent pour relever un chemin partant de $\tilde{x}$. Ensuite on applique le lemme 7.4 avec $Y = [0,1]$. □

Ces lemmes permettent de montrer la proposition suivante

Proposition 7.7. *Soit $p : \tilde{X} \to X$ un revêtement. Soit $x \in X$ et $\tilde{x} \in \tilde{X}$. Le groupe fondamental $\pi_1(\tilde{X}, \tilde{x})$ de $\tilde{X}$ est isomorphe à un sous-groupe du groupe fondamental $\pi_1(X, x)$ de X.*

Démonstration. Cette proposition découle directement des lemmes de relèvement des chemins et des homotopies. □

L'idée est ensuite de montrer que, lorsque X vérifie certaines propriétés (analogues au fait qu'une extension soit galoisienne), tout sous-groupe de $\pi_1(X, x)$ correspond à une classe de revêtements isomorphes. Cette construction se fait en partie grâce à la construction de ce qu'on appelle le revêtement universelle de X. C'est un espace topologique dont le groupe fondamental est trivial ($\langle 1 \rangle$). En mettant tous les résultats ensemble, on montre que si X est connexe par arcs et localement connexe, alors il y a une correspondance entre l'ensemble des classes de conjugaisons des sous-groupes de $\pi_1(X)$ et l'ensemble des classes d'équivalences des revêtements de X.

8 Conclusion

L'esprit de la théorie de Galois est d'associer des groupes (groupes topologiques, ou des invariants etc...) à des objets que l'on peut ordonner (des extensions L/K, des revêtements etc...). Lorsque l'objet en question vérifie certaines propriétés (être galoisien), la structure forte des groupes permet de classer les sous-objets, car chacun est lui-même doté de son propre groupe, qui peut être vu comme un sous-groupe du groupe associé à l'objet initial. Ce point de vue montre toute la modernité des idées de Galois.

En théorie de Galois classique, nous avons montré la correspondance entre les corps intermédiaires à une extension galoisienne L/K et l'ensemble des sous-groupes de $\mathrm{Gal}(L/K)$. La nature même du groupe permet de déduire si le polynôme qui génère l'extension est résoluble par radicaux ou non. Nous avons ensuite calculé le groupe de Galois général d'un extension cyclotomique de $\mathbb{Q}$ - le terrain de jeu historique des mathématiciens - et avons montré comment la géométrie associée à la constructibilité à la règle et au compas pouvait s'interpréter en terme de théorie des corps, puis en terme de théorie de Galois. La théorie de Galois infinie ne fait que prolonger la correspondance galoisienne au cas des extensions algébriques de degré infini. Cette théorie offre l'avantage de donner des outils pour étudier une infinité d'extensions algébriques "d'un seul coups" grâce au théorème fondamental de la théorie de Galois infinie et à la structure de groupe profini du groupe de Galois. Pour le chapitre sur la théorie de Galois en théorie algébrique des nombres, nous nous sommes intéressé à l'action du groupe de Galois d'un extension galoisienne L/K sur des sous-ensembles de L. En particulier, sur l'anneau des entiers O_L de L et ses idéaux. Cela permet de mieux connaître les liens entre l'arithmétique du corps de base K et l'arithmétique sur L. De manière tout à fait analogue à la condition nécessaire et suffisante de résolubilité d'une équation polynomiale par radicaux, nous avons vu que la nature même du groupe de Galois différentiel de l'extension de Picard-Vessiot d'une équation différentielle $Y' = AY$ permet de savoir si l'équation différentielle est résoluble par des fonctions élémentaires ou non. Enfin, la théorie de Galois trouve une théorie tout à fait analogue dans l'étude des revêtements des espaces topologiques. Si ces théories semblent toutes assez différentes, elles sont toutes liées, d'une part via l'esprit de la théorie de Galois, d'autre part, parce que même la théorie des revêtements possède des applica-

tions en théorie de Galois différentielle et, comme pour la théorie de Galois infinie, en théorie de Galois inverse.

Références

[1] Şaban Alaca et Kenneth S Williams. *Introductory algebraic number theory*. Cambridge University Press Cambridge, 2004.

[2] Mark Anthony Armstrong. *Basic topology*. Springer Science & Business Media, 2013.

[3] Emil Artin et Arthur Norton Milgram. *Galois theory*. T. 2. Courier Corporation, 1998.

[4] Helmut Bender, George Glauberman et Walter Carlip. *Local analysis for the odd order theorem*. T. 188. Cambridge University Press, 1994.

[5] Frederick Michael Butler. « Infinite galois theory ». Thèse de doct. Citeseer, 2001.

[6] Antoine Chambert-Loir. *Algebre corporelle*. Éditions École Polytechnique, 2005.

[7] Keith Conrad. « Infinite Galois theory (draft) ». In : (2002).

[8] Évariste Galois. *Oeuvres mathématiques d'Évariste Galois*. Gauthier-Villars et fils, 1897.

[9] Allen Hatcher. *Algebraic topology*. aaa, 2005.

[10] John M Howie. *Fields and Galois theory*. Springer Science & Business Media, 2007.

[11] John H Hubbard et Benjamin E Lundell. « A first look at differential algebra ». In : *The American Mathematical Monthly* 118.3 (2011), p. 245-261.

[12] Neal Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta-Functions*. T. 58. Springer Science & Business Media, 2012.

[13] Jerald J Kovacic. « An algorithm for solving second order linear homogeneous differential equations ». In : *Journal of Symbolic Computation* 2.1 (1986), p. 3-43.

[14] Alain Kraus. *Théorie de Galois. Cours accéléré de DEA*. 1998.

[15] Michio Kuga. *Galois' Dream : Group Theory and Differential Equations : Group Theory and Differential Equations*. Springer Science & Business Media, 2012.

[16] Serge Lang et al. *Algebra*. Springer New York, 2002.

[17] Yves Laszlo. *Introduction à la théorie de Galois*. les Éd. de l'École polytechnique, 2013.

[18] Haoran Liu. « Infinite Galois Theory ». In : (2016).

[19] Andy R Magid. *Lectures on differential Galois theory*. 7. American Mathematical Soc., 1994.

[20] Gunter Malle et Bernd Heinrich Matzat. *Inverse Galois Theory*. Springer, 1999.

[21] James S Milne. *Fields and Galois theory*. 2020.

[22] Patrick Morandi. *Field and Galois theory*. T. 167. Springer Science & Business Media, 2012.

[23] Jürgen Neukirch. *Algebraic number theory*. T. 322. Springer Science & Business Media, 2013.

[24] Thomas Peterfalvi. *Character theory for the odd order theorem*. T. 272. Cambridge University Press, 2000.

[25] Jean-Pierre Ramis. *A short introduction to differential Galois theory*. Rapp. tech. 1988.

[26] Joseph Rotman. *Galois theory*. Springer Science & Business Media, 1998.

[27] Joseph J Rotman. *An introduction to algebraic topology*. T. 119. Springer Science & Business Media, 2013.

[28] Pierre Samuel. « Théorie algébrique des nombres ». In : (1967).

[29] Igor Rostislavovich Shafarevich. « Construction of fields of algebraic numbers with given solvable Galois group ». In : *Izvestiya Rossiiskoi Akademii Nauk. Seriya Matematicheskaya* 18.6 (1954), p. 525-578.

[30] Ian Stewart et David Tall. *Algebraic number theory and Fermat's last theorem*. CRC Press, 2015.

[31] Ian Nicholas Stewart. *Galois theory*. CRC press, 2015.

[32] John Swallow. *Exploratory Galois Theory*. Cambridge University Press, 2004.

[33] René Taton et Évariste Galois. « Les relations d'Évariste Galois avec les mathématiciens de son temps ». In : *Revue d'histoire des sciences et de leurs applications* (1947), p. 114-130.

[34] Marius Van der Put et Michael F Singer. *Galois theory of linear differential equations*. T. 328. Springer Science & Business Media, 2012.

[35] Helmut Volklein et Volklein Helmut. *Groups as Galois groups : an introduction*. 53. Cambridge University Press, 1996.

[36] Lawrence C Washington. *Introduction to cyclotomic fields*. T. 83. Springer Science & Business Media, 1997.

[37] Steven H Weintraub. *Galois theory*. Springer Science & Business Media, 2008.